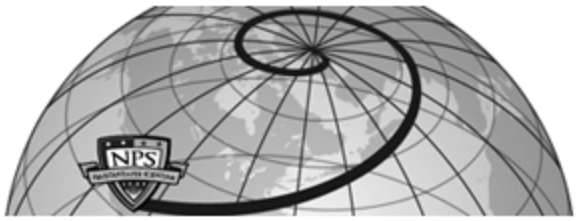

UMD-LM-14-012

Addressing Counterfeit Parts in the DoD Supply Chain

By:
Jacques S. Gansler, William Lucyshyn, and John Rigilano

Center for Public Policy and Private Enterprise
School of Public Policy

March 2014

This research was partially sponsored by a grant from
The Naval Postgraduate School

University of Maryland 18 56

The Center for Public Policy and Private Enterprise at the University of Maryland's School of Public Policy provides the strategic linkage between the public and private sector to develop and improve solutions to increasingly complex problems associated with the delivery of public services—a responsibility increasingly shared by both sectors. Operating at the nexus of public and private interests, the Center researches, develops, and promotes best practices; develops policy recommendations; and strives to influence senior decision-makers toward improved government and industry results.

Table of Contents

Executive Summary

Counterfeit parts have the potential to cause a serious disruption to Department of Defense (DoD) supply chains, delay ongoing missions, and affect the integrity of weapons systems (Government Accountability Office [GAO], 2010). Incredibly, the number of counterfeit parts in electronic military systems more than doubled between 2005 and 2008, rising from 3,868 incidents to 9,356 incidents (U.S. Department of Commerce, 2010). The range of counterfeited goods is wide, and it is growing. The rise of e-commerce, extended international supply chains, stronger reliance on overseas manufacturing, and, more recently, the global economic recession have significantly contributed to the proliferation of counterfeit goods ("Knock Offs Catch On," 2010). Almost anything can be counterfeited, including fasteners used on aircraft and materials used in body armor and engine mounts. In some instances, lives may be at stake.

Today, technology development and production are globally dispersed. As a result, the U.S. defense industrial base has undergone a sea change in its composition, becoming increasingly reliant on international sources for its development, production, and provision, particularly at the subsystems and parts levels. Non-U.S. firms are major players within the U.S. defense industrial base, often with major engineering and production subsidiaries in the United States. Both U.S. and non-U.S. defense firms have rapidly and dramatically increased their reliance on foreign suppliers, especially for the acquisition of commodities, circuit boards, semi-conductors, and other electronic parts and components. In fact, virtually all U.S weapons systems manufactured today contain foreign parts. This arrangement has allowed the United States to acquire superior systems, reduce costs, increase the number of units produced, and improve deployment times (Moran, 1990). But it has also heightened supply chain vulnerability.

If the proliferation of global defense firms and suppliers presents risks, so does the consolidation of the U.S. defense industrial base. A string of defense firm mergers in the 1990s resulted in significant industry consolidation. The number of major U.S.-based defense and aerospace companies shrunk from 21 in 1993 to six today.

This consolidation (which included considerable vertical integration, with the primes absorbing many of the suppliers) also had an impact at the lower levels, with many of the remaining

suppliers moving much of their business to the commercial sector. These suppliers could no longer rely on the DoD to provide the majority of their business. In many critical defense areas, the number of suppliers remaining—at either the prime contractor or lower-tier levels—is down to only one or two. This smaller network of trusted global suppliers can lead to difficulties in acquiring parts, especially replacement parts that are no longer manufactured by the original producer. As a result, the defense industry must look to foreign suppliers with whom it has no prior relationship.

As far as the DoD is concerned, counterfeit electronic components merit greatest concern. In 2012, the Committee on Armed Services uncovered overwhelming evidence of large numbers of counterfeit parts making their way into critical defense systems. According to the report, the investigation "exposed a defense supply chain that relies on hundreds of unvetted independent distributors to supply electronic parts for some of our most sensitive defense systems" (Committee on Armed Services, 2012, p.1). Between 2009 and 2010, the investigation uncovered 1,800 cases of suspect counterfeit electronic parts, with the total number of individual suspect parts exceeding more than a million. Suspect counterfeit parts were discovered in critical weapons systems, including Navy helicopters and Air Force cargo jets.

Counterfeit electronics may take the form of functional knock-offs made in chip factories that pirate the designs of other chips. More commonly, counterfeiters apply fake markings to lower quality or less sophisticated chips in an effort to pass them off as more expensive chips.

It can be especially challenging to ensure that the acquired electronic components are genuine, given this industry's relatively quick innovation cycles. Many active military systems were built using now-obsolete components, the production of which was halted years, even decades, ago by the original manufacturer. This creates a business opportunity for vendors to sell "new old stock," which, in turn, creates traction for the manufacture of semiconductors made from recycled, broken, fake, or otherwise inauthentic parts.

Various industries have developed rigorous counterfeit detection and prevention processes. For instance SAE International, an aerospace industry group, developed an anti-counterfeit standard that requires, notably, that companies complete a risk assessment, and provide for external

auditing, ongoing testing and inspection, supply chain traceability, and penalties associated with fraud (SAE, 2013). The standard is intended to inform individualized requirements that are commensurate with program risk, and are intended to be "flowed down" through the supply chain by all organizations that procure electronic parts. The requirements are to be enforced via contract specifications (SAE, 2013).

NASA was the first government agency to adopt SAE International AS5553 on November 3, 2008, before the official release of the plan (NASA, 2013). The DoD followed suit in August 2009, requiring that the standard be used for internal purchasing purposes; however, the DoD does not require that its contractors adhere to this specific standard.

The pharmaceuticals industry is another leader in the development of rigorous anti-counterfeit processes. For example, tamper-evident packaging using plastic seals, outside lids, and seals between lids and containers protect consumer medicines. Recently, The U.S.-Member Body for the IEC Quality Assessment System for Electronic Components discussed the potential use of tamper-evident packaging for sensitive electronic parts and components, noting that it might provide "a level of confidence when dealing with returns" and thus has the potential for lowering handling costs (Salot, 2011).

The pharmaceutical industry also uses track and trace technologies, which allow companies to determine the current and past locations of items. However, the use of these technologies present challenges. For instance, the significant costs associated with implementation can prove problematic. Moreover, there is no single, interoperable technology upon which all parties rely.

The DoD faces similar challenges. In November 2012, the DoD began using plant DNA to mark microcircuits. The DNA can be mixed with inks or infused into the actual materials like silicon, plastics, and wires (Freedberg, 2012). But DNA tagging does not eliminate the problem of currently circulating counterfeit parts in secondary markets. Moreover, because the DoD is not the largest buyer of microelectronics, the private sector market must buy into DNA tagging in order for manufacturers to include this anti-counterfeit measure on all products.

The DoD has not adopted the aerospace standard, nor has it developed its own. And given the difficulty in establishing uniform track and trace processes, as well as the uncertaintly regarding the value of tamper-evident packaging and other technologies, the DoD has come to rely primarily on contractor reporting, the development of trusted networks of suppliers, and, to a lesser extent, the testing of parts and components in order to reduce the incidence of counterfeiting.

On a legislative front, Section 818 of the National Defense Authorization Act (NDAA) for Fiscal Year 2012 (enacted in December 2011) contains new mandates for the DoD to mitigate the threat of counterfeit electronic parts. Of most note, Section 818 stipulates that contractors "who supply electronic parts or products … are responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts." Also significant, the law stipulates that the DoD and all DoD contractors and subcontractors must "whenever possible" obtain electronic parts from original equipment manufacturers (OEMs) or their authorized dealers, or from "trusted suppliers" that obtain parts exclusively from OEMs or their authorized dealers. Finally, the law also required contractors and subcontractors to report counterfeit parts using the Government Industry Data Exchange Program (GIDEP) or some other designated counterfeit reporting system.

Section 818 also called for establishing department-wide definitions of the terms ''counterfeit electronic part,'' and directed DoD programs to implement a risk-based approach to minimize the impact of counterfeit electronic parts or suspect counterfeit electronic parts on the Department (NDAA for Fiscal Year 2012). Also of note, the law called for the revision of guidance on remedial actions to be taken in the case of a supplier who has repeatedly failed to detect and avoid counterfeit electronic parts.

The DoD has proposed to amend the Defense Federal Acquisition Regulation Supplement (DFARS) in order to meet some of these requirements. Final action is expected in early 2014. The proposed DFARS addresses some ongoing problems but creates new challenges. This supplement was supposed to be released for comment by September 2012 but was delayed by more than seven months. Contractors were dismayed to learn that, according to the guidance, firms had to devise their own "acceptable counterfeit electronic parts avoidance and detection

systems" (DFARS, 2012). Insofar as the guidance prescribed specific processes and procedures, it was wholly inadequate. In addition, the new guidance failed to adequately refine the definition of trusted supplier and made no mention of the role that the DoD, or other government customer, would play (if any) with regard to source approval. Again, given that liability rested solely with the contractor, this shortcoming in the DFARS was perceived as unfair by many within the contractor community.

This approach is not consistent with the DoD's internal practices. Regarding the DoD's own purchasing practices, Section 818 directs the DoD to implement a risk-based approach in an effort to prevent the inclusion of counterfeit parts (NDAA for Fiscal Year 2012). Metzger (2013) noted that by describing an approach as "risk-based," the DoD has tacitly acknowledged that "it is impossible to eliminate all risk of counterfeit in every system that the DoD buys or supports" (p. 3). Thus, Metzger (2013), Livingston (2013), and others conclude that contractor liability should be limited to some extent based on the "best efforts" of contractors to avoid the inclusion of counterfeit parts.

Another problem is that the definition of counterfeit part contained in the DFARS (2012)) includes what, in the commercial sector, would be described simply as "nonconforming." According to subparagraph 3 of the new DFARS rule, a counterfeit part includes items "misrepresented by any source to the end-user as meeting the performance requirements for the intended use." Livingston (2013) noted that this definition could include "an out of spec item due to a temporary lapse of manufacturing and testing process control" (p. 5).

Although the DFARS guidance is deficient in some respects, some of the criticism aimed at the supplement is clearly ill advised. According to the supplement, firms that are not subject to cost accounting standards because of their smaller size are not required by law to establish and maintain a detection and prevention system. Representatives of large firms have taken aim at this exception, pointing out that because the vast majority of suppliers associated with the sale of suspect counterfeit parts are small, lower-level sub-contractors, independent distributors, or brokers, the law should require that these entities maintain anti-counterfeit systems.

Of course, large contractors can and should require their subcontractors and suppliers to take steps to avoid counterfeit parts and may go so far as to hold these lower-tier entities partially or fully liable for remediation in the event that counterfeit parts are discovered. Moreover, the flow down of anti-counterfeit measures is already a component of the SAE standards and is one of the elements of an adequate counterfeit detection system per Section 818 (NDAA, 2011). Large firms, it might be argued, were seeking a legal mandate in order to avoid the legwork of establishing flow-down requirements, monitoring subcontractors and suppliers, and ensuring compliance.

It appears that Congress has come to realize that the incidence of counterfeit parts cannot be fully eliminated. Section 833 of the 2013 NDAA includes amendments to Section 818, allowing a contractor to seek reimbursement for the cost of counterfeit remediation provided that it has an approved operational system to detect and avoid counterfeit parts.

The threat of counterfeit parts within the DoD's supply chain is real. We can anticipate that that threat will only escalate over time, with potentially serious consequences. The DoD must address the threat of counterfeit parts in the supply chain; however, the solutions must take into account the budgetary constraints that the department faces and will likely continue to face for some time. It is critical that the DoD find an appropriate and acceptable balance between risks and costs.

This balance is reflected in the recommendations provided below, which fall into three high-level categories: (1) strengthen standards, (2) implement stronger preventive measures, and (3) develop a long-term strategy.

<u>Strengthen Standards</u>

- The DoD should require contractors to rely on recognized standards, such as SAE AS5553, in devising its counterfeit detection and mitigation procedures.

- DoD program managers should partner with program contractors to determine an appropriate, individualized, risk-based approach to counterfeit mitigation that adheres to established standards.

- The DoD should enforce quality assurance standards, recognizing that nonconforming parts threaten weapons system integrity and may lead to costly remediation.

Implement Stronger Preventive Measures

- The DoD should, where appropriate, encourage the use of existing deterrents (e.g., tamper-proof packaging, x-ray inspection) while developing new anti-counterfeiting technologies.

- Debar suppliers who repeatedly furnish parts or components containing counterfeit parts.

- The DoD should require foreign companies to report suspect counterfeits using GIDEP, and provide penalties for non-compliance.

Develop a Long-Term Strategy

- The DoD should focus on best value, as opposed to lowest cost, in its acquisition of critical technologies.

- The DoD should minimize the impact of obsolescence by using (to the extent possible) parts and components for which multiple sources exist. Where this is not possible, the DoD must develop a robust obsolescence management strategy.

- The United States should strive to retain its design capabilities for critical technologies.

The threat of counterfeit parts within DoD's supply chain is real and will only escalate over time, with potentially serious consequences. In order to reduce this threat, the DoD and its industry partners will have to work together to reduce the risk to acceptable levels, at an affordable cost. While both parties may have the best intentions, it is essential that any incentives, penalties, and rewards be properly aligned in order to produce the desired outcome.

I. Introduction

In 2011, the Department of Defense (DoD) discovered that counterfeit memory chips had made their way into computers controlling America's primary missile defense system, the Terminal High Altitude Area Defense System (THAAD; Johnson, 2012a). The discovery reignited debate among DoD officials, members of Congress, and defense industry groups over liability for counterfeit parts in weapons systems, a contentious issue that has received more attention over the last decade as defense contractors have worked to expand their networks of global suppliers—some of whom, it appears, cannot be trusted.

During a congressional hearing, Michigan Senator Carl Levin asserted that "there is no reason on earth that the replacement of a counterfeit part should be paid for by American taxpayers, instead of by the contractor who put it in a military system" (Johnson, 2012a, p. 1). Pentagon officials tended to agree, and in the case of the THAAD, charged the primary contractor, Lockheed Martin, for replacement costs totaling $2.7 million.

At first glance, holding contractors responsible for the remediation of counterfeit parts in DoD systems seems reasonable enough, especially considering that the high cost of remediation serves an essential purpose: to incentivize contractors to establish more rigorous policies and procedures to prevent counterfeit parts from entering their supply chains.

In today's budgetary environment, however, both government agencies and contractors face continuous pressure to reduce costs while improving performance and reliability. Implementing new supply chain security mandates while attempting to reduce acquisition costs will pose a challenge. Under the 2012 National Defense Authorization Act (NDAA), DoD contractors are already required, whenever possible, to purchase parts and components from the original manufacturers (either the original equipment manufacturer [OEM] or the original component manufacturer [OCM]), their authorized dealers, or "trusted suppliers," a term that has yet to be adequately defined. As a result, contractors have had to establish separate supply chains—those upon which they rely for government business and those that they use to meet their commercial business needs. Needless to say, the narrowing of supply chains has led to increased costs that

contractors pass along to their government customers, an outcome that is seemingly at odds with the DoD's current spending reduction priority.

It is projected that the DoD will see a funding reduction of $487 billion over the next 10 years (Office of Management and Budget [OMB], 2012). Moreover, the Congressional Budget Office (CBO) found that the DoD's 2013 Future Years Defense Program (FYDP), a five-year spending plan provided to Congress, fails to bring down spending to a sustainable level. In fact, the CBO believes that the DoD's costs will soon outstrip its budget as expenditures for manpower, maintenance, and healthcare continue to increase, thereby eliminating the funds necessary for the planned recapitalization, modernization, and transformation of the military (CBO, 2013). The DoD must make hard decisions in order to prevent such an outlook from becoming a reality. With regard to counterfeit detection and prevention, reaching an appropriate balance between risks and costs is critical.

Unfortunately, recent approaches to reducing costs may be having the opposite effect. The DoD's increased use of lowest price technically acceptable (LPTA) source selection criteria—according to which the government agency awards the contract to the offeror submitting the lowest price proposal that meets the technical requirements—may indirectly encourage the inclusion of counterfeit parts followed by costly remediation. Larry Allen, the president of consulting firm Allen Federal Business Partners, put it this way: "While contractors should not be off the hook, the government can't expect to pay discount prices for real stuff or real product" (Johnson, 2012a, p. 18).

Sometimes lost in the debate is the fact that counterfeit parts and components can greatly affect the safety, operational readiness, cost, and critical nature of the military mission. Counterfeit parts have the potential to cause a serious disruption to DoD supply chains, delay ongoing missions, and even affect the integrity of weapons systems (Government Accountability Office [GAO], 2010). Almost anything can be counterfeited, including fasteners used on aircraft, electronics used in missile guidance systems, and materials used in body armor and engine mounts. In some instances, lives may be at stake.

As mentioned, the DoD's sourcing supply chain, like that of any other large enterprise, has become increasingly global. The DoD procures millions of parts through its logistics support providers—Defense Logistics Agency (DLA) supply centers, military service depots, and defense contractors—who are responsible for ensuring the reliability of the DoD parts that they procure. Never an easy task, the challenge of assuring the integrity and provenance of parts and components has grown geometrically more complex in this global sourcing environment. Visibility into supplier operations is often quite limited, quality controls are insufficient, and chain of custody verification is lacking.

Additionally, as DoD weapons systems age, products required to support them may no longer be available from the original manufacturers or through franchised or authorized suppliers. Instead, the DoD must turn to independent distributors, brokers, or aftermarket manufacturers as sources of supply. Here again, the DoD is at risk for acquiring counterfeit parts. Counterfeiters, for their part, have developed more sophisticated capabilities in recent years, making detection all the more difficult. This much, then, is clear: in this environment, the DoD must step up its war against counterfeit parts.

Report Roadmap

This report will provide a thorough exploration of the issue of counterfeit parts within the defense supply chain. We begin in Part II by discussing the impact of the rapid globalization of the defense industry on the proliferation of counterfeit parts. In Part III, we describe various manifestations of counterfeiting in the commercial sector, with particular emphasis on electronic parts and components. Then, we assess the current and potential threat of counterfeit parts infiltrating the DoD's acquisition chain, including analyzing areas of highest vulnerability and risk. Next, in Part IV, we analyze how some industries (e.g., pharmaceuticals and aerospace) address the counterfeit parts issue, reviewing successful best practices and counterfeiting-prevention models and processes. In Part V, we review DoD efforts to mitigate this threat across the acquisition cycle, within the services and defense agencies. We also explore the challenges involved in implementing anti-counterfeiting procedures across the DoD's supply chain. Finally, in Part VI, we present our recommendations and discuss potential barriers to success.

II. Evolution of the Defense Industry

The emergence of a global defense industrial base has allowed the DoD to take advantage of increased competition and innovation, leading to the acquisition of superior systems that are more affordable. However, as a consequence of globalization, the U.S. has grown more dependent on offshore sources for defense-related technologies, especially in critical, lower tier component areas. The proliferation of counterfeit parts and components in DoD systems, broadly speaking, can be significantly attributed to the rapid globalization of the defense industry.

Entrance of the Commercial Sector

Before and during the Cold War, much of the nation's research and development investment was concentrated on defense. The resultant technologies (e.g., jet propulsion, satellites, and computers) were then adapted ("spun off") to civilian and commercial applications. The end of the Cold War was coincident with the start of the information revolution, and research investments began to focus on commercial applications. There was also a significant increase in the global investment in research and development (R&D), so that now it is greater than the total U.S. investment (see Figure 1).

	Cold War (1965)	**End of Cold War (1993)**	**2009**
U.S. Government	$60B	$75B	$80B
U.S. Commercial	$90B	$200B	$300B
Rest of World	Unknown	$300B	$450B

Figure 1. R&D investment
Note. The information in this figure comes from the Army Science Board (2013).

The entrance of the commercial sector into advanced information technology R&D created another option for the defense industry to consider when purchasing and adapting systems and technology for military use. In 1999, the Defense Science Board (DSB) concluded that

> the commercial sector, which pays scant attention to national boundaries, is now driving the development of much of the advanced technology integrated into modern information-intensive military systems. This is especially true of the Software and

> consumer microelectronics sectors. Accordingly, U.S. military-technological advantage will derive less from advanced component and subsystem technology developed by the U.S. defense sector than from the military functionality generated by superior, though not necessarily U.S.-based, defense sector systems integration skills. (p. 8)

The commercial sector continues to invest heavily in developing and advancing technologies, often outpacing similar work performed by the defense industrial base. As early as 1986, upon the publication of the President's Blue Ribbon Commission on Defense Management report ("the Packard Commission"), it was clear that commercial technologies regularly outperformed their "MIL-SPEC" counterparts, and that they could be procured at far lower costs. The availability of high-quality, commercial off-the-shelf (COTS) hardware and software has netted significant savings to the DoD, in terms of systems development and maintenance (McKinney, 2001). It is clear that the vector of technology transfer has reversed, and defense increasingly strives to adapt the latest commercial developments and products.

Proliferation of Global Defense Firms

The formerly segregated defense industries of Western countries have begun to transform themselves into a global, more commercially oriented industry. They have done so through consolidations, mergers, acquisitions, joint ventures, and integrations that cross national boundaries. It should be noted that the globalization of the defense industry began at both ends—by U.S. defense firms seeking foreign markets, and by foreign defense firms seeking an entry into the largest of all markets for defense goods, the United States.

During the infancy of the semiconductor industry, a single company performed specification, design, manufacturing, and testing (Villasenor, 2013). As the technology evolved, and the semiconductors became smaller and more complex, the costs of in-house manufacturing became prohibitive. As is the case in many industries, it became cheaper for a company to send design specifications to an external facility that would manufacture semiconductors for multiple entities, thereby capturing economies of scale and reducing production costs. As a result, semiconductor technology continues to evolve, leading to the production of ever-advancing systems that are

superior to their predecessors. However, semiconductors are among the electronic parts that are most prone to counterfeiting and other forms of manipulation.

Today, technology development and production are globally dispersed. As a result, the U.S. defense industrial base has undergone a sea change in its composition, becoming increasingly reliant on international sources for its development, production, and provision. Non-U.S. firms are major players within the U.S. defense industrial base, often with major engineering and production subsidiaries in the U.S. Both U.S. and non-U.S. defense firms have rapidly and dramatically increased their reliance on foreign suppliers, especially for the acquisition of commodities, circuit boards, semi-conductors, and other electronic parts and components.

The defense industry's reliance on foreign suppliers reflects a growing trend that cuts across virtually all industries. The number of U.S. companies that source internationally has increased dramatically over the last 40 years. According to Trent and Roberts (2010), total purchases from non-U.S. sources by U.S. firms have increased from less than 10% of total purchases in the early 1990s to more than 25% in 2000. Today, the figure likely stands at around 20% (Trent & Roberts, 2010). The increase in international purchasing can be attributed to the growing competitive pressure to lower costs in order to realize larger profits. This pressure, once constrained by geographic and then national boundaries and trade embargos, has evolved into a global force.

In 2012, 20 aerospace and defense firms made the Forbes Global 2000 List of the largest public companies operating in the global market. Eleven of these firms have their headquarters based outside of the United States (see Figure 2), including BAE Systems, EADS, and Thales. Foreign firms have increasingly established themselves as part of the U.S. aerospace and defense industry. By purchasing U.S. companies or establishing U.S. subsidiaries, these foreign defense companies have gained a significant foothold in the largest defense market in the world, contributing in large part to the domestic U.S. economy.

These firms regularly compete alongside Lockheed Martin, Northrop Grumman, and Boeing for contracts with the U.S. government. Moreover, these companies often work with each other across national boundaries. As a result, the U.S. relies, and must continue to rely, on multiple

firms, foreign and domestic that, in turn, rely on multiple, disparate networks of suppliers. More often than not, this arrangement has led to the U.S. acquisition of superior systems while allowing the DoD to reduce costs, increase the number of units produced, and improve deployment times (Moran, 1990). But it has also heightened supply chain vulnerability.

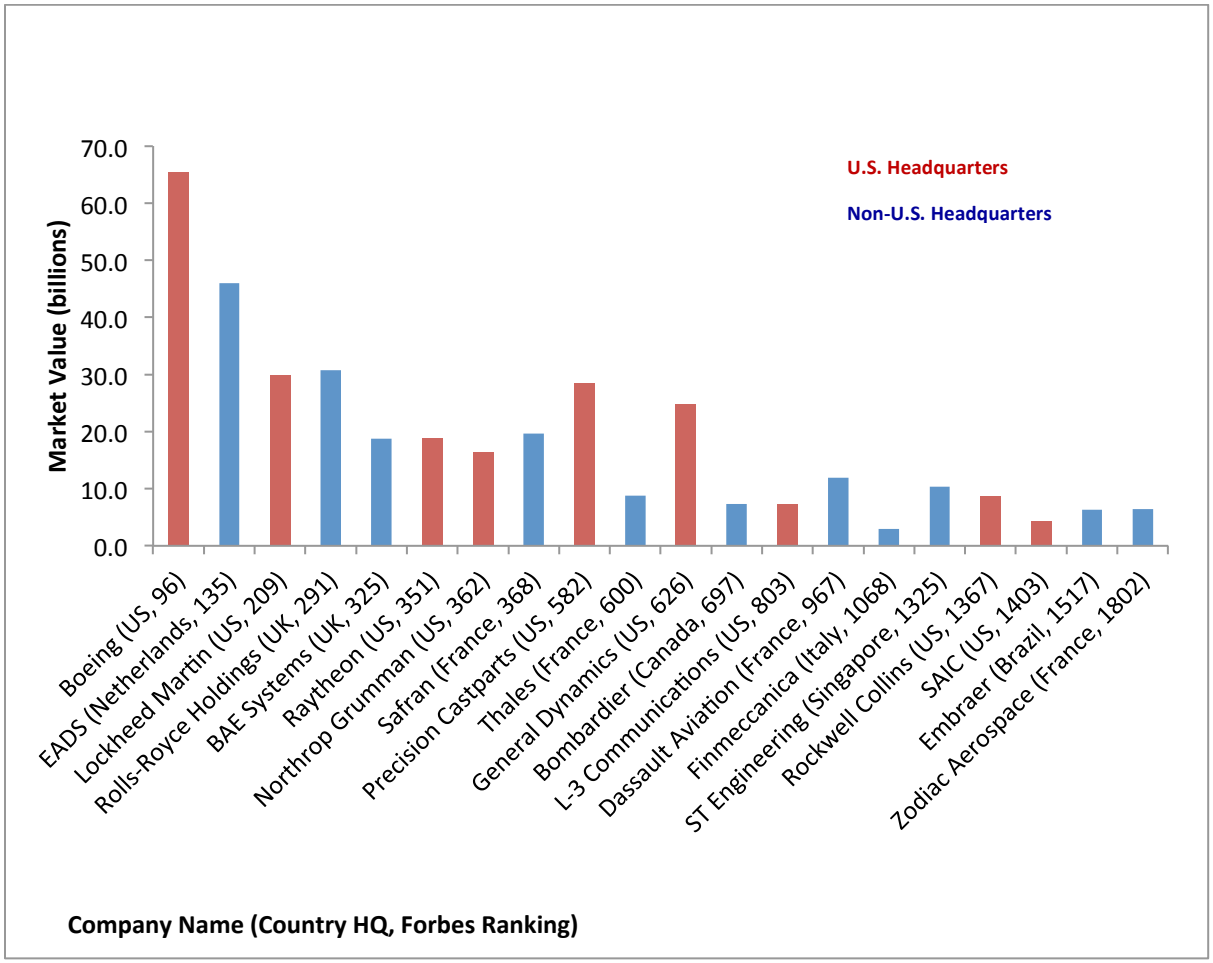

Figure 2. Market value of the largest global public aerospace and defense companies
Note. The information in this figure came from Forbes (2013).

Industry Consolidation

If the proliferation of global defense firms and suppliers presents risks, so does the consolidation of the U.S. defense industrial base. A string of defense firm mergers in the 1990s resulted in significant industry consolidation. The number of major U.S.-based defense and aerospace companies shrunk from 21 in 1993 to six today.

This consolidation (which included considerable vertical integration, with the primes absorbing many of the suppliers) also had an impact at the lower levels, with many of the remaining suppliers moving much of their business to the commercial sector. These suppliers could no longer rely on the DoD to provide the majority of their business. In many critical defense areas, the number of suppliers remaining—at either the prime contractor or lower-tier levels—is down to only one or two. The smaller network of trusted suppliers can lead to difficulties in acquiring parts, especially replacement parts that are no longer manufactured by the original provider. Often, the DoD must look to foreign or commercial suppliers with whom it has no prior relationship.

In April 2013, the Pentagon acknowledged that it had leased a Chinese satellite to provide urgently needed communications capabilities for its Africa command. The DoD stated that the Chinese satellite provides "unique bandwidth and geographic requirements" that other satellites do not (Capaccio, 2013). China is Africa's largest trading partner, and Chinese companies (Huawei and ZTE in particular) have invested significantly in the continent's infrastructure; the construction of an advanced communications satellite is but one investment among many. From an economic standpoint, the arguments in favor of the U.S. leasing the Chinese satellite are clear: it provides superior performance that cannot easily be obtained from other providers, and it was readily available in a time of urgent need.

Globalization of the defense industry is already well underway and largely irreversible. Indeed, virtually all U.S weapons systems manufactured today contain foreign parts. Yet objections to "buying foreign" are voiced repeatedly within American defense circles, wasting valuable time and resources. Congress, industry, and the public regularly scrutinize DoD decisions to buy or lease foreign parts or entire systems, collaborate on projects with oversees partners, or share technology with allies, regardless of the details. To be sure, there are risks associated with globalization, including the purchase of counterfeit parts, which is precisely why the United States must pursue a defense industrial policy that anticipates, rather than reacts to, the expansion of global trade and technological innovation.

III. Counterfeits: A Growing Problem

The practice of counterfeiting is growing, but it is not new. Daniel Hamermesh (2013) pointed to a display of shrunken heads, once prepared by Amazon tribes for trophy or ritual purposes, that is featured at the Mutter Museum in Philadelphia. The display includes the following explanation:

> Westerners traveling to the territory in the late 19th century … were fascinated with the heads and offered the tribe money and guns in exchange … This led to an increase in warfare…both to get more heads to sell and because of the prevalence of guns. It also led to the creation of counterfeit heads … made from real human heads but not prepared by the tribe, and others [that] were made from monkey, goat, or other animal skin. (Hamermesh, 2013, p. 1)

Similar schemes exist today. Some lower-tier subcontractors and suppliers for major defense companies will go as far as to manufacture or otherwise procure authentic parts, only to mix them with older and often cheaper parts of inferior quality and/or non-working parts. Needless to say, schemes of this sort make determining the provenance of counterfeit parts and components exceedingly difficult.

Counterfeit Consumer Goods

Counterfeiters strike when the costs are low and the rewards are high, hence their interest in industries such as fine wine and pharmaceuticals. It is relatively easy to remove and replace wine labels. And many people cannot distinguish between a $15 and $50 bottle of wine, let alone between a $300 and a $1,000 bottle of wine, the price range that many wine counterfeiters tend to deal in. It is not until they get careless that they are caught. In 2012, a California man was charged with trying to sell a wine bottle that he claimed was a 1929 Domaine Ponsot. However, Domaine Ponsot did not begin bottling until 1934. Similarly, pharmaceuticals are targeted by counterfeiters because the manufacturing costs are so low—reproducing the authentic-looking packaging is more expensive than making the fake drug.

But not all counterfeiters are looking for an immediate payoff. Counterfeiting takes many forms, with those responsible constantly devising new schemes. In October of 2012, for example, hundreds of crates of Heinz ketchup were discovered in an abandoned warehouse in Dover, New Jersey (Kim, 2012). Many of the bottles had exploded due to the heat. Authorities also found several empty bottles, labels, and equipment. Apparently, bottles of "Simply Heinz" ketchup—whose retail value is higher than Heinz's traditional ketchup—were being emptied and refilled with traditional Heinz. Though authorities have yet to conclude their investigation, it appears that counterfeiters were looking to pull one over on consumers. Though the ketchup never reached stores, the counterfeiters stood to make a 36-cent premium for each bottle of the not-so-premium ketchup sold.

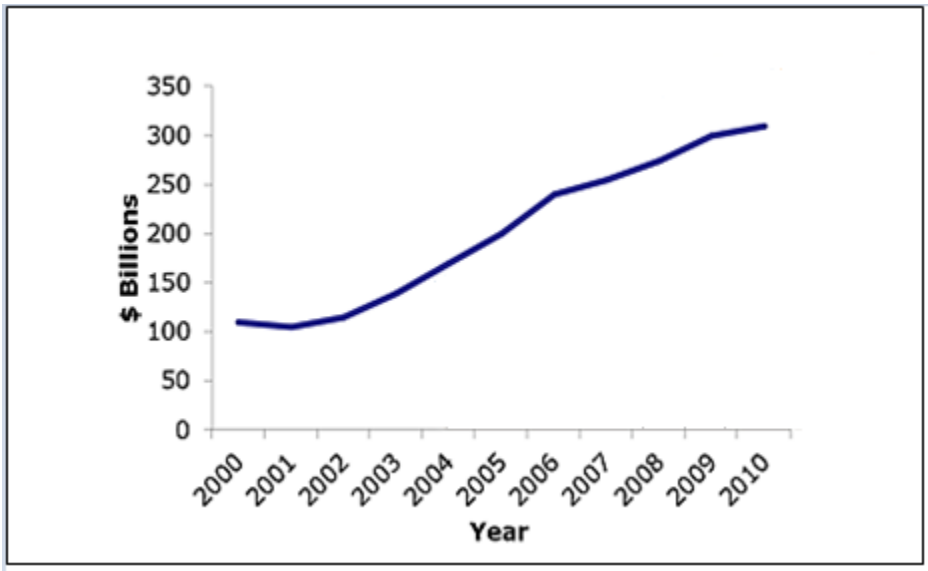

Figure 3. Global economic impact of counterfeit consumer goods
Note. The information in this graph is from OECD (2011).

The range of counterfeited consumer goods is wide, and it is growing (see Figure 3). The rise of e-commerce, extended international supply chains, stronger reliance on overseas manufacturing, and more recently, the global economic recession, have all contributed to the proliferation of counterfeit goods ("Knock Offs Catch On," 2010). In addition to the many smaller goods, such as watches, purses, cigarettes, movies, and software, the consumer market has seen a marked increase in the counterfeit production of luxury cars and motorcycles.

Counterfeit Electronics

Counterfeiting operations run the gamut, from swapping ketchup labels to the sophisticated reproduction of advanced electronics. Somewhere in the middle of this continuum resides the burgeoning practice of harvesting and, often, repurposing electronic waste or "e-waste" (e.g., discarded computers, office electronic equipment, entertainment device electronics, mobile phones, telephones, and refrigerators). Even the poorest of the poor can engage in this practice. In the slums of China, India, and Pakistan, peasants "cook" circuit boards over trash can fires in order to remove the metal chips, selling them to local counterfeiting operations (see Figure 4). A 2008 article in *Bloomberg* describes the "garbage-strewn streets" of Guiyu, in Guangdong Province, China, as reeking of "burning plastic as workers in back rooms and open yards strip chips from old PC circuit boards" (Grow, Chi-Chu, Edwards, & Burnsed, 2008, p. 2).

Once the chips are cleaned, refurbished, and relabeled, they are purchased by unscrupulous military subcontractors that go on to supply "military grade" microchips to many of America's largest defense companies. These microchips have been found in American weapons systems. The threat of counterfeit parts continues to grow as counterfeiters have developed more sophisticated capabilities to replicate parts and gain access to scrap materials that were thought to have been destroyed (Belva, 2010).

Figure 4. A woman in Taizhou, China, melts a circuit board to remove the metal chips (Basel Action Network, 2007)

Counterfeits may also take the form of functional knock-offs made in chip factories that pirate the designs of other chips. More commonly, counterfeiters apply fake markings to lower quality or less sophisticated chips in an effort to pass them off as more expensive chips (see Figure 5).

Figure 5. This chip was coated and remarked. The original logo is partially visible. (AERI, 2013)

Counterfeit chips may show signs of having been manipulated. These signs include discoloration, dirt, or residues on the leads; non-uniform color; no exposed copper on the ends of leads; missing pins; excessive or uneven plating; and excessive solder on leads (SAE, 2013). Discrepant markings are also characteristic of counterfeit parts. For example, devices marked with the same date and/or lot code may exhibit varying country-of-origin stamps, body molds, and backside markings (SAE, 2013). Sometimes, previous marking may be visible on the device's surface. Often, in an effort to remove markings, counterfeiters sand down the chip and then resurface it. However, counterfeiters may not always succeed in replicating the indentations formed during the initial molding process (see Figure 6).

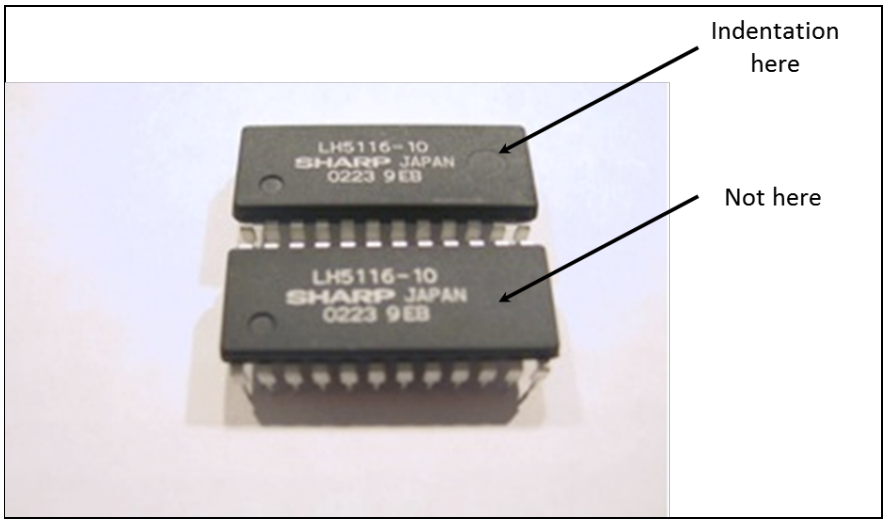

Figure 6. A legitimate chip (top) and a non-working counterfeit chip (AERI, 2013)

According to the National Aeronautics and Space Association (NASA), which has led the way in establishing industry standards for counterfeit detection and prevention, there are several factors that have drawn counterfeiters to the electronic component market. These factors include the following (Oberhettinger, 2008):

- Device obsolescence has caused an increase in the scarcity and price of critical components used in military and civil aerospace systems.
- The flow of information through internet product search engines facilitates finding obsolete or hard-to-find devices, and obtaining delivery overnight or within a few days. But internet purchases may provide no traceability or complex part sourcing history, minimal warranties, and no certainty of replacements or refunds.
- With the increasing sophistication and complexity of component technology, it may be more difficult to detect fakes. Testing of incoming items has decreased over the years, resulting in a reliance on the suppliers' Certificate of Compliance as proof of authenticity and compliance.
- Unauthorized gray market channels for legitimate products can facilitate distribution by counterfeiters. Gray market distributors cannot determine whether a high volume influx of a product is a counterfeit or a legitimate OCM product that has been redirected from the source.

- Subcontract assemblers and manufacturers may not report suspect devices in order to protect their reputation for quality.

Villasenor (2013) pointed out that today's computer chips have become so complex that it is virtually impossible for a single individual to understand every element of its design. Consequently, quality assurance through automated testing is next to impossible as "it would take many years to exhaustively test everything that a modern large chip can do" (Villasenor, 2013, p. 2). Accordingly, testing is performed on a statistical basis using only a small fraction of possible inputs that are observed and used to infer proper functionality for inputs not specifically tested. Clearly, having to rely on inference rather than evidence of functionality is problematic. In 2005, The Defense Science Board (DSB) stated that "trust cannot be added to integrated circuits after fabrication; electrical testing and reverse engineering cannot be relied upon to detect undesired alterations in military circuits" (p. 3).

Damaged, recycled, and inferior electronic chips may show signs of "undesired alteration," which may or may not lead a weapons system to improperly function. However, there is greater—and growing—concern that some electronic chips are intentionally altered during the design process. In his paper, "Compromised by Design? Securing the Defense Electronics Supply Chain," Villasenor (2013) wrote that "as chips have gotten more complex … the opportunities to insert malicious functionality have increased" (p. 1). Moreover, Villasenor (2013) asserts that the "attacker" need not have advance knowledge of the chip's destination: "An attacker could afford to cast a wide net, knowing that only a tiny fraction of corrupted chips would end up in systems of interest" (p. 9). In other words, the attacker could design a small "back door" in every system, the majority of which would never be exploited.

Reporting Counterfeits

Government agencies as well as private companies are encouraged to report counterfeits using several databases. The first is the Government Industry Data Exchange Program (GIDEP). The GIDEP serves as a data repository for the collection and sharing information on nonconforming parts and materials (Livingston, 2010). This web-based database allows government and industry participants to share information on deficient parts, including counterfeits.

A GIDEP user can submit information on a suspected counterfeit part, and GIDEP policy allows for up to 15 days for the supplier to respond before posting this information to the database. To ensure that reports are objective and fact based, GIDEP policy requires submitters to notify suppliers of their intention to report. All parties involved are allowed to present their side of the story (Belva, 2010).

Although GIDEP is the predominant counterfeit reporting mechanism in place for government and its suppliers, it is not universally utilized. A study by the Aerospace Industries Association [AIA] of America (2012) found several reasons why some suppliers do not use the system, including "legal or liability issues" (e.g., exposure to third-party lawsuits) that encumber reporting and organizations' business processes that do not "support reporting non-conforming material findings outside of the organization" (AIA, 2011, p. 13).

The GIDEP issued an interim policy change regarding "Reporting Suspect Counterfeit Parts and Materials" in September 2010 to "facilitate and encourage the reporting of suspect counterfeits until such time as federal policy and an appropriate supporting procedure can be determined and implemented" (AIA, 2011, p. 13). Under the current GIDEP policy, members are asked to identify the supplier of the part or material when reporting a suspect counterfeit in the database (AIA, 2011).

However, GIDEP members are sometimes "hesitant or not permitted to identify the supplier due to potential legal issues or other concerns" (p. 13). If the "true" manufacturer or supplier is not identified when submitting a report, "current GIDEP policy limits the use … to only a Problem Advisory" and prevents the "reporter from alerting the community via a Safe-Alert or Alert when the severity or likelihood of the failure is known" (AIA, 2011, p. 13).

The DoD also uses the Joint Deficiency Reporting System (JDRS), a cross-service, web-enabled, automated tracking system designed to initiate, process, and track deficiency reports, in addition to the Product Data Reporting and Evaluation Program (PDREP) for reporting and disposal of deficient parts. JDRS and PDREP do not have a specific field in which to report counterfeit parts. Some DoD officials stated that they report suspect counterfeits to internal fraud teams;

others indicated that they would contact local law enforcement or the Federal Bureau of Investigation in similar cases.

Additionally, agencies within the DoD have taken specific actions to block the flow of counterfeit products. For example, the DLA's Defense Supply Center Columbus (DSCC) implemented a Qualified Suppliers List of Distributors (QSLD) program (U.S. Department of Commerce, 2010).

The purpose of the QSLD program is to establish and maintain a list of pre-qualified sources for certain electronic components that are purchased and managed by DLA Land and Maritime. QSLD products are provided by suppliers that combine accepted commercial practices, quality assurance procedures that are consistent with industry and international quality standards, and tailored when necessary to product-unique requirements that can take the place of provisions traditionally stated in DLA Land and Maritime solicitations (DLA, 2012).

This approach is designed to reduce the need for testing, engineering reviews, and other activities that can delay acquisitions and increase acquisition costs. The QSLD program also enables the DSCC to use automated electronic parts purchasing, but with a modification from past practice. All purchases made through the QSLD system are subject to a final manual review prior to execution. About 50% of parts would be acquired through the system, enabling the DSCC to reassign some personnel to other duties (U.S. Department of Commerce, 2010).

Counterfeits in Department of Defense Systems

The same global forces responsible for the increase in consumer counterfeits have also impacted the aeronautics and defense industries. Across the DoD, counterfeits of all types—from electronic equipment to metal fasteners—have been found. As a direct consequence, the lives of military men and women are at stake. Incredibly, the number of counterfeit parts in electronic military systems more than doubled between 2005 and 2008, rising from 3,868 incidents to 9,356 incidents (U.S. Department of Commerce, 2010).

Thus far, the impact of counterfeit parts in the supply chain has been minimal in this regard. According to Pentagon Press Secretary George Little, "[the DoD] is unaware to date of any loss

of life or catastrophic mission failure that has occurred because of counterfeit parts" (Ferran, 2012, p. 1). But given the massive growth if counterfeit parts in the supply chain, it may only be a matter of time. Accordingly, the DoD has remained resolute in its approach. Little has also stated, "We will not stop until we strengthen our efforts to identify, prevent and detect these smaller pieces of equipment from entering our supply chain" (p. 1).

In a 2010 report, the U.S. Department of Commerce defined a counterfeit as a part that is not genuine because it

- is an unauthorized copy;
- does not conform to original component manufacturers (OCMs) design, model, and/or performance standards;
- is not produced by the OCM or is produced by unauthorized contractors;
- is an off-specification, defective, or used OCM product sold as new or working; or
- has incorrect or false markings and/or documentation.

All branches of the services are affected by the threat of counterfeit parts. The following examples illustrate cases in which counterfeit parts have infiltrated the services' supply chains (GAO, 2010):

Army—Seatbelt clasps: Seatbelt parts were made from a grade of aluminum that was inferior to that specified in DoD's requirements. The parts were found to be deficient when the seatbelts were accidentally dropped and they broke.

Navy—Routers: The Navy, as well as other DoD and government agencies, purchased counterfeit network components—including routers—that had high failure rates and the potential to shut down entire networks. A two-year FBI criminal investigation led to 10 convictions and $1.7 million in restitution.

Air Force—Microprocessor: The Air Force needed microprocessors that were no longer produced by the original manufacturer for its F-15 flight-control computer. These microprocessors were procured from a broker, and F-15 technicians noticed additional markings on the microprocessor and character spacing inconsistent with the original part. A total of four

counterfeit microprocessors were found and, as a result, were not installed on the F-15s' operational flight control computers.

Defense Logistics Agency—Packaging and small parts: During a two-year period, a supplier and three co-conspirators packaged hundreds of commercial items from hardware and consumer electronics stores and labeled them as military-grade items. For example, a supplier labeled the package containing a circuit from a personal computer as a $7,000 circuit for a missile guidance system. The suppliers avoided detection by labeling packages to appear authentic, even though they contained the wrong part. The supplier received $3 million from contracts totaling $8 million before fleeing the country.

In June 2007, the Bureau of Industry and Security's (BIS's) Office of Technology Evaluation (OTE) conducted a defense industrial base assessment of counterfeit electronics. OTE surveyed five segments of the supply chain including the original component manufacturers (OCMs), distributors and brokers, circuit board assemblers, prime contractors and subcontractors, and DoD agencies. The report came to the following conclusions:

> OTE data revealed that 39 percent of companies and organizations participating in the survey encountered counterfeit electronics during the four-year period. Moreover, information collected highlighted an increasing number of counterfeit incidents being detected, rising from 3,868 incidents in 2005 to 9,356 incidents in 2008. The rise of counterfeit parts in the supply chain is exacerbated by demonstrated weaknesses in inventory management, procurement procedures, recordkeeping, reporting practices, inspection and testing protocols, and communication within and across all industry and government organizations. (U.S. Department of Commerce, 2010, p. i)

The study revealed several key reasons why counterfeits enter the DoD supply chain. Figure 7 lists the top 10 reasons.

Greater reliance by brokers on gray market parts	42%
Greater reliance by independent distributors on gray market parts	37%
Less stringent inventory management by parts brokers	36%
Less stringent inventory management by independent distributors	28%
Insufficient buying procedures	23%
Insufficient chain of accountability	27%
Purchase of excess inventory on the open market	23%
Inadequate part purchase planning by OEMs	23%
Inadequate part purchase planning by contract manufacturers	23%
Greater reliance on contract manufacturers for procurement	23%

Figure 7. Top 10 reasons for counterfeits entering the supply chain (U.S. Department of Commerce, 2010)

As Figure 7 demonstrates, the DoD's increasing reliance on so-called gray market parts explains, in large part, the growing supply of counterfeits. The booming gray market in military-grade electronics in particular emerged for a number of reasons, including the DoD's persistent need for aging equipment, and, more recently, declining budgets—smaller brokers settle for smaller profit margins. In addition, federal law has encouraged the DoD to favor smaller, disadvantaged, suppliers (e.g., minority or veteran owned; Grow et al., 2008), which may rely on less secure practices. Today, the DoD procures millions of parts through its logistics support providers. As they draw from a large network of suppliers in an increasingly global supply chain, there can be limited visibility into these sources. These sources include the original component manufacturers, independent distributors, brokers, or aftermarket manufacturers (see Figure 8).

Type of Source	Description
Original component manufacturer (OCM)	Organization that designs, or engineers, a part and is pursuing or has obtained the intellectual property rights to that part.
Franchised distributor	Distributor with which OCM has a contractual agreement to buy, stock, repackage, sell, and distribute its product lines.
Independent distributor	Distributor that purchases new parts with the intention to sell and redistribute them back into the market, and which does not have contractual agreements with OCM.
Broker/ broker distributor	In the independent distribution market, brokers are professionally referred to as independent distributors. A broker distributor is a type of independent distributor that works in a just-in-time environment by searching the industry and locating parts for customers.
Aftermarket manufacturer	Manufacturer that either (1) produces and sells replacement parts authorized by the OCM, or (2) produces parts through emulation, reverse-engineering, or redesign that match OCM specifications and satisfy customer needs without violating OCM intellectual property rights, patents, or copyrights.

Figure 8. Types of DoD suppliers of parts and components (Belva, 2010)

As mentioned, aging systems often rely on obsolete parts and components. As DoD weapons systems age, products required to support it may no longer be available from the original manufacturers or through franchised or authorized suppliers. Moreover, DoD logistics offices in charge of solving obsolescence problems are challenged by limited budgets and time constraints. According to a report by the Department of Commerce (2010), "it is typically less expensive to find part substitutions and aftermarket manufacturing [i.e. "built-to-print" shops] for needed electronic parts than reengineering and redesigning parts and components. In addition, obsolescence mitigation strategies also take a long time to implement" (p. 1). As a result, procurement agents must purchase parts from unknown sources; this, of course, heightens the risk of acquiring counterfeit parts.

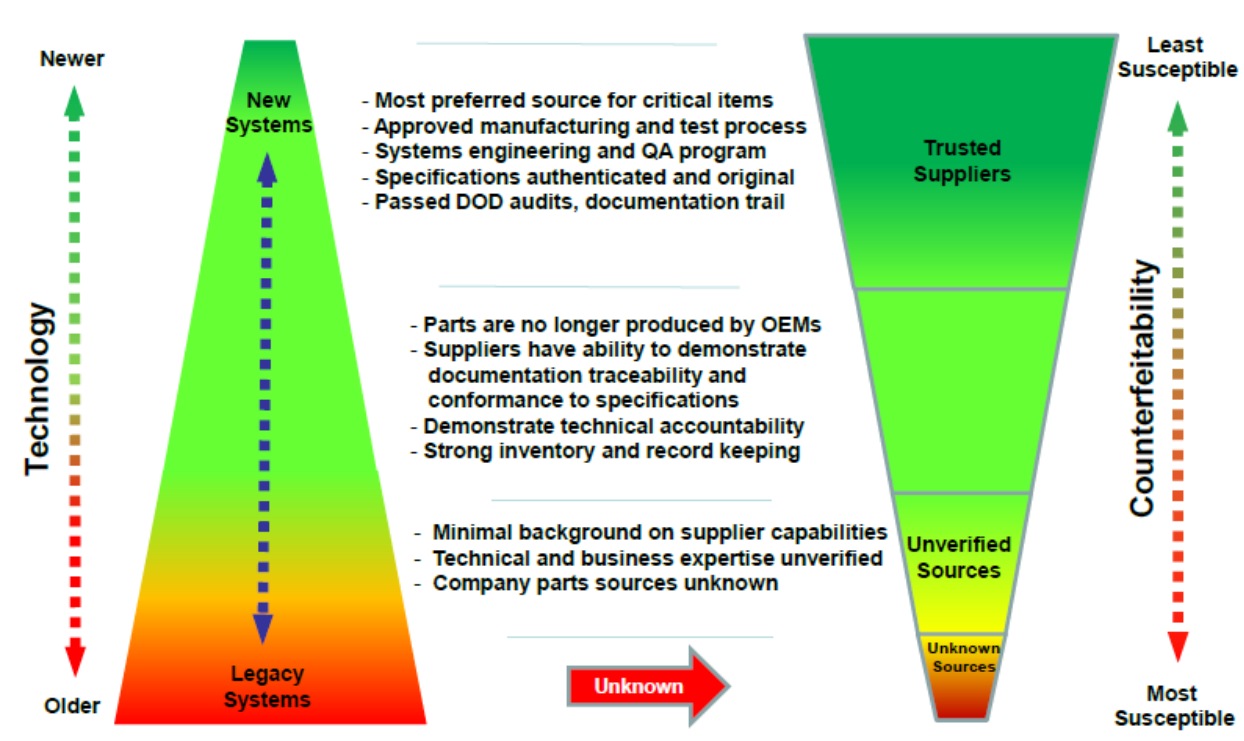

Figure 9. Aging systems are associated with an increased risk of acquiring counterfeit parts (Peters, 2012)

It is especially challenging to acquire legitimate semiconductors given this industry's relatively quick innovation cycles. Hamermesh (2013) described the counterfeit shrunken heads as a case of "induced supply push" (p. 1). Because there was unmet demand for shrunken heads, new sellers entered the market selling replicas. In the case of semiconductors, many active military systems were built using now-obsolete semiconductors, the production of which was halted years, even decades, ago by the original manufacturer. This creates a business opportunity for vendors to sell "new old stock," which, in turn, creates traction for the manufacture of semiconductors made from recycled, broken, fake, or otherwise inauthentic parts. Figure 9 illustrates the association between aging systems (i.e., "legacy" systems) and the risk to the DoD of acquiring counterfeit replacement parts.

IV. Counterfeit Detection and Prevention

Counterfeiting in any industry threatens innovation by reducing the value of intellectual property. However, counterfeit wines and ketchup do not pose the same risks as counterfeit aerospace components or pharmaceuticals, for obvious reasons. As a result, these two industries have designed rigorous and effective detection and prevention processes in order to mitigate risk. We examine these processes in the sections that follow.

Aerospace

In 2007, SAE International chartered a committee to develop standards for counterfeit detection and prevention for the aerospace industry. SAE is a U.S.-based, globally active professional association and standards organization for engineering professionals. The organization coordinates the development of technical standards based on best practices identified and described by SAE committees. The committee formed with representatives from the U.S. Department of Homeland Security, the DoD, NASA, original component manufacturers, contract assembly manufacturers, distributors, and industry suppliers and associations. This committee worked to develop a counterfeit electronic parts control plan known as SAE International AS5553 ("Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition"), which it formally released in April 2009.

In 2009, the committee developed a document that standardized requirements, practices, and methods related to counterfeit parts risk mitigation. The committee also developed a counterfeit electronic parts control plan that includes processes to specifically address counterfeit part risk mitigation methods in areas including electronic design and parts management, supplier management, procurement, part verification, material control, and response strategies when suspect or confirmed counterfeit parts are discovered (Johnson, 2012b)). The plan, SAE International Standard AS5553, was entitled "Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition." SAE (2013) described the new standard as follows:

> The resulting product presents solutions in addressing counterfeit electronic parts issues across a large cross section of the electronics industry by requiring those who adopt it to develop and implement a counterfeit electronic parts control plan. The control plan

> includes processes to specifically address counterfeit part risk mitigation methods in electronic design and parts management, supplier management, procurement, part verification, material control, and response strategies when suspect or confirmed counterfeit parts are discovered. (p. 2)

The standard requires, notably, that companies complete a risk assessment and provide for external auditing, ongoing testing and inspection, supply chain traceability, and penalties associated with fraud (SAE, 2013). The standard is intended to inform individualized requirements that are commensurate with program risk and are intended to be "flowed down" through the supply chain by all organizations that procure electronic parts. The requirements are to be enforced via contract specifications (SAE, 2013).

NASA was the first government agency to adopt SAE International AS5553 on November 3, 2008, before the official release of the plan (NASA, 2013)). The DoD followed suit in August 2009, requiring that the standard be used for internal purchasing purposes; however, the DoD does not require that its contractors adhere to this specific standard.

Identification, removal, and prevention of counterfeit electronics in NASA's supply chain is critical to maintaining the safety of personnel and the integrity of components used in satellites, rockets, communications systems, and computers. As is the case with DoD, counterfeit parts can threaten missions and, more importantly, lives. For this reason, NASA goes to exhausting lengths to ensure component quality and integrity.

To implement the policy, NASA focuses on educating and training its people and its suppliers. The agency provides awareness briefings, reports all ERAI counterfeit parts alerts to all NASA organizations, and hosts bi-annual quality leadership forums and annual supplier quality conferences. Training includes (1) a review of the Independent Distributors of Electronics Association (IDEA) Inspection Standard 1010A to all NASA centers and prime contractors; (2) a course in Counterfeit Parts Avoidance for inspectors, operators, auditors, and suppliers; and (3) an AS5553 course and training module (Zulueta, 2011).).

One example of NASA's efforts to eradicate quality issues and preempt counterfeit risk is the Goddard Space Flight Center (GSFC) supplier assessment program. The GSFC selects each prime contract supplier for an assessment every two years. Lower tier supplier assessment considerations include high-risk or critical suppliers, common supplier for multiple mission projects, new suppliers, supplier issues or concerns elevated to senior management, or a project office request. The assessment includes a review of procedures and processes, sampling of documents or records, interviews of management and personnel, and direct observation.

From this review, the assessment team generates a report that includes corrective and preventive actions. Then, the report is distributed to the supplier, NASA GSFC offices, and other NASA centers or agencies (Root, 2011).

During execution of the corrective and preventive action plan, the NASA team performs a root-cause analysis and a cost-benefit analysis of corrective actions. The team also determines timing and assesses short- and long-term containment actions. Finally, the team works with the facility to implement corrective and preventive actions based on priority, impact, and risk (Brunello & Robinson, 2011). As a result of supplier assessments at GSFC, the team addresses issues such as obsolete procedures referenced, expired materials, logs not correct or not signed/dated, calibration supplier contract inadequate, and mishap reporting not accurate (Sivcovich, 2012).

NASA's Dryden Flight Research Center relies on five testing phases and inspections in order to ensure against counterfeits (Johnson, 2012b). Contractors are required to document the parts that they use, and parts are inspected and tested before flight. Contractors then receive a weighted risk score ranging from one to 100. A score of 52 qualifies a contractor to do business with NASA (Johnson, 2012b).

NASA has mandated (1) supply chain traceability to the OCM or aftermarket manufacturer that identifies the name and location of all of the supply chain intermediaries from the part manufacturer to the direct source of the product for the seller, and (2) flow down of applicable requirements of this document to applicable contractors and their subcontractors (Zulueta, 2012).

The National Aeronautics and Space Administration (NASA) Authorization Act of 2010 emphasized the improvement of NASA's efforts against counterfeits (Zulueta, 2011). NASA's success in reducing counterfeit electronics by adopting SAE International AS5553 catalyzed the formation of a new multi-agency working group. In 2010, 14 U.S. government agencies, including Intellectual Property Enforcement Coordinator (IPEC), Office of Management and Budget (OMB), DoD, NASA, Department of Energy (DoE), and General Services Administration (GSA), formed the USG Inter-Agency Anti-Counterfeiting Working Group to identify areas of common interest and compare progress and best practices to ultimately eliminate counterfeits in their supply chains and develop a consistent and effective government-wide approach to reducing the U.S. government's vulnerability to counterfeit products (Executive Office of the President of the United States , 2011).

NASA has begun to focus on the education of its suppliers through sharing current policy and requirements with suppliers, sending out new electronic component surveys to assess risk level, and narrowing down the specifics of what qualifies as a "trusted supplier" (Foster, 2012).

Pharmaceuticals

The World Health Organization (WHO; 2013) defines a counterfeit pharmaceutical product as

> a counterfeit medicine is one which is deliberately and fraudulently mislabeled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products, and counterfeit products may include products with the correct ingredients or with the wrong ingredients, without active ingredients, with insufficient active ingredients or with fake packaging.

In poor countries that lack the necessary safety precautions, or where government inspectors can be easily bribed, counterfeit drugs are ubiquitous. In Nigeria, for example, over 60% of antimalarial drugs are fakes. The majority (over 70%) of these often useless (and sometimes even deadly) drugs originate from India and China (WHO, 2011). Luckily, counterfeit drugs are rare in the United States, thanks to the relatively high level of safety assuredness for U.S. pharmaceuticals (Lechleiter, 2012). However, serious incidents have occurred.

Today, pharmaceutical companies take additional precautions to prevent this type of incident. Anti-counterfeit technologies in the pharmaceutical industry fall into three major categories: (1) tamper-evident or tamper-resistant packing, (2) product authentication, and (3) track and trace technology.

Tamper-evident and tamper-resistant packaging was one of the first forms of anti-counterfeit technologies. In the fall of 1982, Johnson & Johnson was forced to respond when seven patients died after taking cyanide-laced Tylenol in the Chicago area. The company conducted a voluntary, nation-wide recall and provided free replacements for all of its consumers. When the company re-released the product, Tylenol was available only in new tamper-proof containers.

Tamper-evident packaging can include plastic seals outside lids and seals between lids and containers. Although the use of tamper evident closures does not make a product tamper-proof, it can give consumers peace of mind that the products they are buying have not been altered after leaving the manufacturer. Recently, The U.S.-Member Body for the IEC Quality Assessment System for Electronic Components discussed the potential use of tamper-evident packaging for sensitive electronic parts and components, noting that it might provide "a level of confidence when dealing with returns" and thus has the potential for lowering handling costs (Salot, 2011).

The pharmaceutical industry also uses product authentication measures, which rely on overt, covert, and forensic features to prevent counterfeit production. Holograms and color shift inks are examples of overt features, while digital watermarks and invisible printing are examples of covert features. Forensic features include biological and chemical tags (see Figure 10).

Features	Overt features	Covert features	Forensic features
Examples	Holograms, colour-shift Inks	Embedded images, digital watermarks, invisible printing	Chemical and biological tags, microtaggants
Advantages	User verifiable, more secure, decorative appeal, low cost	Easily added or modified, need regulatory approval, applied in-house or via component suppliers, low cost	High-tech and secure against copying, provide positive authentication, may be disclosed for overt purposes
Dis-advantages	Require user education, easily mimicked, rely on covert features for authentication, may be re-used or refilled, provide false assurance	Need strict secrecy, risk of compromise, more secure options add supply complexity and cost	Licensed technologies, significant cost, difficult to implement and control across many markets, unlikely to be available to authorities or public

Figure 10. Comparison of pharmaceutical product authentication characteristics

Newer technologies include the Sproxil authentication system and SecureLight+. The Sproxil authentication system has a scratch-off label with a unique code. Consumers can send a free text message with the code to Sproxil, and the system responds with another free text informing the consumer whether the product is genuine. This system already has been implemented in Nigeria. SecureLight+ instantly changes color under both compact fluorescent light (CFL) and LED light sources, allowing the confirmation of authenticity. SecureLight+ has an additional safeguard that contains an up-converting infrared feature and a customizable digital signature that can be read only with a specifically tuned handheld device (see Figure 11).

The pharmaceutical industry also relies on track-and-trace technologies, which allow companies to determine the current and past locations of items. Radio-frequency identification and barcodes are two common technology methods used to provide traceability. Within the pharmaceutical industry, “e-pedigree” numbers or codes track all the way through the supply chain, allowing companies to confirm that a product is authentic from the time it leaves the manufacturing site to the time it hits the shelves.

However, track and trace technologies are not the panacea that many manufacturers claim. For instance, RFID use comes with risks, such as damage to biotechnology products (due to

electromagnetic waves). Moreover, the significant costs associated with implementation can prove problematic. According to Barlas (2008), "it is the pharmacies, more than the manufacturers or the wholesalers, that have the more complex technical task and that face the higher cost hit, based on percentage of revenues" (p. 1). He went on to state that

> the big revenue hit would come from the need to purchase various types of bar code readers, radio frequency identification (RFID) chip readers, and software and database upgrades so that pharmacies will be able to authenticate each individual package from the bar code or the RFID chip (or both) attached to each package label. (Barlas, 2008, p. 1)

Moreover, there is no single, inter-operative e-Pedigree technology upon which all parties rely, and e-Pedigree laws are in a constant state of flux. For these reasons, the Food and Drug Administration (FDA) has yet to mandate the use of a universal track-and-trace system.

Company Name	Technology	Description	(Country) Patent Number
Microsoft Corporation	Labels using randomly-occurring features	Pattern unique to each label	(US) 7,878,398
Axsun Technologies	Taggants read using Raman spectroscopy	Can be made unreadable by chemical modification	(US) 7,875,457
CSEM SA (Centre Suisse d'Electronique et de Microtechnique) (Swiss firm)	Zero-order diffractive pigments (ZOPs)	Produce very pronounced colours that can't be copied	(US) 7,864,424
AlpVision (Swiss firm)	Cryptoglyph invisible marking technology	Invisible signature on package	(India) 243454 (Indonesia) P0025514B
PANalytical BV (Dutch firm)	Use of angle-dispersive X-ray diffraction	Compared to reference signatures in data library	(US) 7,756,248

Figure 11. Patented anti-counterfeit technologies

The DoD faces similar challenges. In November 2012, the DoD began using plant DNA to mark microcircuits. SigNature DNA security measures are manufactured by Applied DNA Sciences in

Stony Brook, New York (Winter, 2013). Each item bears an individual plant's DNA sequence that has been altered slightly from its natural state, preventing accidental marking or confusion with naturally occurring plant DNA (Winter 2013). This altered DNA can be mixed with inks or infused into the actual materials like silicon, plastics, and wires (Freedberg, 2012).

But DNA tagging does not eliminate the problem of currently circulating counterfeit parts in secondary markets. Moreover, because the DoD is not the largest buyer of microelectronics, the private sector market must buy in to DNA tagging in order for manufacturers to include this anti-counterfeit measure on all products.

The DoD has not adopted the aerospace standard, nor has it developed its own. And given the difficulty in establishing uniform track and trace processes as well as uncertaintly regarding the value of tamper-evident packaging and other technologies, the DoD has come to rely primarily on contractor reporting, the development of trusted networks of suppliers, and, to a lesser extent, the testing of parts and components in order to reduce the incidence of counterfeiting. The DoD's policies and and initiatitives are explored in the next section.

V. Addressing Counterfeits in Defense Systems

In 2012, the Committee on Armed Services released its *Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain*. The inquiry was launched partially in response to a 2010 GAO report that concluded that the

> DoD is limited in its ability to determine the extent to which counterfeit parts exist in its supply chain because it does not have a department-wide definition of the term counterfeit and a consistent means to identify instances of suspected counterfeit parts. (p. 21)

The extensive report issued by the committee uncovered overwhelming evidence of large numbers of counterfeit parts making their way into critical defense systems. It also revealed failures by contractors and the military services and DoD agencies to report the occurrence of counterfeits. According to the report, the investigation "exposed a defense supply chain that relies on hundreds of unvetted independent distributors to supply electronic parts for some of our most sensitive defense systems" (Committee on Armed Services, 2012, p. 1). Between 2009 and 2010, the investigation uncovered 1,800 cases of suspect counterfeit electronic parts, with the total number of individual suspect parts exceeding more than a million. Suspect counterfeit parts were discovered in critical weapons systems, including Navy helicopters and Air Force cargo jets. The committee came to the following conclusions:

> Conclusion 1: China is the dominant source country for counterfeit electronic parts that are infiltrating the defense supply chain.
>
> Conclusion 2: The Chinese government has failed to take steps to stop counterfeiting operations that are carried out openly in that country.
>
> Conclusion 3: The DoD lacks knowledge of the scope and impact of counterfeit parts on critical defense systems.
>
> Conclusion 4: The use of counterfeit electronic parts in defense systems can compromise performance and reliability, risk national security, and endanger the safety of military personnel.

Conclusion 5: Permitting contractors to recover costs incurred as a result of their own failure to detect counterfeit electronic parts does not encourage the adoption of aggressive counterfeit avoidance and detection programs.

Conclusion 6: The defense industry's reliance on unvetted independent distributors to supply electronic parts for critical military applications results in unacceptable risks to national security and the safety of U.S. military personnel.

Conclusion 7: Weaknesses in the testing regime for electronic parts create vulnerabilities that are exploited by counterfeiters.

Conclusion 8: The defense industry routinely failed to report cases of suspect counterfeit parts, putting the integrity of the defense supply chain at risk.

These conclusions informed new legislation that was written into Section 818 of the 2012 National Defense Authorization Act (NDAA). This section summarizes Section 818, its implementation, and some of the new challenges that it has created.

Section 818 of the 2012 National Defense Authorization Act

On a legislative front, Section 818 of the National Defense Authorization Act of 2012, enacted in December 2011, contains new mandates for the DoD to mitigate the threat of counterfeit electronic parts. Of most note, Section 818 stipulates that contractors "who supply electronic parts or products … are responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts." Additionally, the new law asserts that "the cost of counterfeit electronic parts and suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are not allowable costs under Department contracts."

Also significant, the law stipulates that the DoD and all DoD contractors and subcontractors must "whenever possible" obtain electronic parts from OEMs or their authorized dealers or from "trusted suppliers" that obtain parts exclusively from OEMs or their authorized dealers.

Finally, the law also requires contractors and subcontractors to report counterfeit parts using GIDEP or other designated counterfeit reporting system.

In addition to these new regulations, Section 818 directs the DoD to take action on a number of related issues, following a period of assessment by the secretary of defense, to be carried out within 180 days of the enactment of the NDAA. These "actions after assessment" included the following:

> 1. Establish department-wide definitions of the terms *counterfeit electronic part* and *suspect counterfeit electronic part*, which definitions shall include previously used parts represented as new.
>
> 2. Issue or revise guidance applicable to department components engaged in the purchase of electronic parts to implement a risk-based approach to minimize the impact of counterfeit electronic parts or suspect counterfeit electronic parts on the department, which guidance shall address requirements for training personnel, making sourcing decisions, ensuring traceability of parts, inspecting and testing parts, reporting and quarantining counterfeit electronic parts and suspect counterfeit electronic parts, and taking corrective actions (including actions to recover costs as described in subsection (c)(2)).
>
> 3. Issue or revise guidance applicable to the department on remedial actions to be taken in the case of a supplier who has repeatedly failed to detect and avoid counterfeit electronic parts or otherwise failed to exercise due diligence in the detection and avoidance of such parts, including consideration of whether to suspend or debar a supplier until such time as the supplier has effectively addressed the issues that led to such failures.
>
> 4. Establish processes for ensuring that department personnel who become aware of, or have reason to suspect, that any end item, component, part, or material contained in supplies purchased by or for the department contains counterfeit electronic parts or suspect counterfeit electronic parts provide a report in writing within 60 days to

appropriate government authorities and to the Government-Industry Data Exchange Program (or a similar program designated by the secretary).

5. Establish a process for analyzing, assessing, and acting on reports of counterfeit electronic parts and suspect counterfeit electronic parts.

March 2012 Memorandum

Initial implementation of the DoD's actions following their assessment began in March of 2012. A memorandum was issued by the under secretary of defense for acquisition, technology, and logistics (USD[AT&L]) to the secretaries of the military departments and directors of the defense agencies. The actions contained in the memo primarily addressed subparagraph 2, above (i.e., the implementation of the risk-based approach to counterfeit detection and prevention). The memorandum stipulated the following:

1. Program managers (PMs) must ensure that they are notified by the contractors and suppliers—including those below the prime contractor level—when critical items are not obtained from the original equipment manufacturer, original component manufacturer, or an authorized distributor.

2. PMs must evaluate counterfeit risk and implement countermeasures for mission critical components, which are outlined in a July 2011 DoD memorandum entitled "Document Streamlining-Program Protection Plan (PPP)." The PPP should address counterfeit prevention, including what measures will be in place and how the program will mitigate the risk of the insertion of counterfeit parts during operations and maintenance [see Figure 12].

3. Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.246-7003, "Notification of Potential Safety Issues," must be included in solicitations and contracts for (1) repairable/consumable parts for critical safety items; (2) systems and subsystems, assemblies, and subassemblies integral to a system; or (3) repair, maintenance, logistics support, or overhaul services for systems and subsystems, assemblies, subassemblies, and

parts integral to a system. This DFARS clause establishes the actions to be taken concerning nonconformance and deficiencies that could result in a critical safety impact.

4. The GIDEP is designated as the central reporting repository for the DoD for suspected and confirmed counterfeit parts. Contractors, subcontractors, and DoD activities are to report counterfeit parts using the GIDEP's Product Quality Deficiency Reporting process. The counterfeit reports are provided to all GIDEP members and are maintained in an on-line searchable database.

Assessing Vulnerability of Critical Components

The questions below are examples of the kinds of factors that should be considered in evaluating the potential vulnerability of a critical component prior to acquisition.

Where and under what conditions was the system designed?

- Who made significant system-wide design decisions?
- Who has had access to design information?
- How are requirements and specifications for critical components communicated to suppliers?
- How much do suppliers know about how critical their products are to the overall system?

Where and under what conditions were critical components developed?

- For custom components, who made significant design decisions?
- Who has had access to design information?
- Where are critical components fabricated or manufactured?
- Who has had access to fabrication or manufacturing processes?
- What testing of critical components has been conducted? How and where?
- How are critical components shipped?
- How has custody of critical components been managed?

How and where are components assembled and integrated into completed systems?

- What final system testing is conducted?

In addition to the above questions, it is useful to assign a criticality level to the overall project. These levels may include:

Level I: Total mission failure
Level II: Significant/unacceptable degradation
Level III: Partial/acceptable degradation
Level IV: Negligible

Figure 12. Assessing the vulnerability of critical components (Fong, 2011)

Defense Federal Acquisition Regulation Supplement

The 2012 NDAA directed the DoD to establish specific requirements for contractor processes to avoid the inclusion of counterfeit parts (including testing, inspection, training, and so forth). It also directed the DoD to refine the definition of counterfeit parts. The DoD is proposing to amend the DFARS in order to meet these requirements. Final action is expected in early 2014.

This supplement was scheduled to be released for comment by September of 2012 but was delayed by more than seven months. Contractors eagerly awaited the release of the new guidance, believing that the issuance of new processes and procedures, if diligently followed, might limit their liability with regard to the cost of counterfeit remediation. However, the new guidance did not include any detailed procedures. Contractors were disappointed to learn that, according to the guidance, firms had to devise their own "acceptable counterfeit electronic parts avoidance and detection systems." The DFARS required these systems to include the following elements:

- the training of personnel;
- the inspection and testing of electronic parts, including criteria for acceptance and rejection, and processes to abolish counterfeit parts proliferation;
- mechanisms to enable traceability of parts to suppliers;
- the use and qualification of trusted suppliers;
- the reporting of counterfeit electronic parts and suspect counterfeit electronic parts;
- the quarantining of counterfeit electronic parts and suspect counterfeit electronic parts;
- methodologies to identify suspect counterfeit parts and to rapidly determine whether a suspect counterfeit part is, in fact, counterfeit;
- the design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts; and
- the flow down of counterfeit avoidance and detection requirements to subcontractor.

One might recall that these elements constitute little more than a reiteration of the programmatic requirements described in the 2012 NDAA under "actions following assessment." However, it is

unclear if any assessment was actually performed. Clearly, insofar as this guidance prescribes specific processes and procedures, it is wholly inadequate, especially considering that liability was to rest entirely with the contractor. The questions "How?" and "To what extent?" can be applied to each of the above elements. In an article entitled "DoD Counterfeit Parts Rule: So Little After So Long," Robert Metzger (2013) wrote that the new guidance "fails to inform contractors of how they can minimize counterfeit risk" (p. 1). Livingston (2013) asserted that elements from SAE Aerospace Standard AS5553 (described in Part IV) could have been used to inform requirements and define implementation details. Similarly, the DoD could have relied on the March 2012 memorandum (described in the previous section) to inform the policies and procedures of an appropriate avoidance and detection system.

In addition, the new guidance failed to adequately refine the definition of trusted supplier (recall that in the event that a contractor is unable to purchase a part or component from the original source [OEM or OCM], the contractor must acquire it from a "trusted supplier," according to the 2012 NDAA). Yet the guidance offered no instruction with regard to vetting and qualifying such a supplier and makes no mention of the role that the DoD, or other government customer, would play (if any) with regard to source approval. Again, given that liability rested solely with the contractor, this shortcoming in the DFARS was perceived as unfair by many within the contractor community.

Henry Livingston (2013), technical director at BAE Systems, asserted that before the DoD proceeds with its implementation of the DFARS guidance, it should

- define the elements of a contractor's counterfeit electronic parts avoidance and detection system, including the central tenets of counterfeit electronic part prevention recommended by industry subject matter experts;
- describe explicit criteria for the DoD's approval; and
- prepare and publish for public comment "audit guidance" associated with the assessment and approval of contractor counterfeit electronic parts avoidance and detection systems.

Critics of the DFARS might suggest that by failing to define specific criteria for system adequacy, the DoD could assert that a contractor who unknowingly procured counterfeits had failed to implement—in adequate fashion—counterfeit detection and prevention measures, even if the contractor's anti-counterfeit system adhered to the basic elements listed above.

This approach is not consistent with the DoD's internal practices. Section 818 directs the DoD to implement a risk-based approach in an effort to prevent the inclusion of counterfeit parts. Metzger (2013) noted that by describing an approach as "risk-based," the DoD has tacitly acknowledged that "it is impossible to eliminate all risk of counterfeit in every system that the DoD buys or supports" (p. 3). Thus, Metzger (2013), Livingston (2013), and others concluded that contractor liability should be limited to some extent based on the "best efforts" of contractors to avoid the inclusion of counterfeit parts.

Yet, based on Section 818, contractors were liable not only for the cost of replacing a counterfeit part, but also for complete remediation up to and including the disassembly and rebuilding of affected systems. In the case of highly complex weapons systems, these costs could be considerable. And in today's globalized defense industry, it is perhaps unfair to place the burden of total remediation on the contractors who design and manufacture America's weapons systems. Metzger (2013) asserted that

> DoD contractors have some influence over counterfeit prevention risk, to be sure, but they did not create that risk and they do not have absolute authority over requirements or sources, much less the time or funds to insist upon parts with perfect provenance or pedigree. (p. 3)

Indeed, it appears that this zero-tolerance policy with regard to counterfeit parts was misguided. Contractor liability should be limited, provided that rigorous detection and prevention regimes are in place. However, a one-size-fits-all regime is also inappropriate. Depending on the nature of the program, the implementation of a costly prevention policy may be less of a priority. As mentioned, counterfeits—from simple commodities, circuit boards, and semi-conductors to advanced electronics—can endanger lives. But they may also prove benign. The DoD already

categorizes parts and components that are essential to weapons system performance or operation, or the safety of operating personnel, as "critical application items." Extending the risk-based approach to contractors, as opposed to implementing a prescriptive regime, allows the DoD to balance cost with risk. With this in mind, one might view the DoD's failure to establish universal criteria for regime adequacy in a more favorable light.

Recall that the DFARS also sought to refine the definition of counterfeit part. Here again, the DFARS contains some problematic language. According to the DFARS,

> Counterfeit part means—
>
> 1. An unauthorized copy of substitute part that has been identified, marked, and/or altered by a source other than the part's legally authorized source and has been misrepresented to be from a legally authorized source;
> 2. An item misrepresented to be an authorized item of the legally authorized source, or
> 3. A new, used, outdated, or expired item from a legally authorized source that is misrepresented by any source to the end-user as meeting the requirements for intended use. (DFARS 202.101)

Note that the DoD's definition of *counterfeit part* includes what, in the commercial sector, would be described simply as "nonconforming." According to subparagraph 3 of the new DFARS rule, a counterfeit part includes new items "misrepresented by any source to the end-user as meeting the performance requirements for the intended use." Livingston (2013) noted that this definition could include "an out of spec item due to a temporary lapse of manufacturing and testing process control" (p. 5).

The fact that the DFARS conflates the definition of counterfeit with nonconformance calls into question Section 818 policy regarding contractor liability in that prior to its passage, cost-reimbursement for nonconforming parts "could not be denied for reasons other than fraud, lack of good faith, or willful misconduct" (FAR 52.246-3(h)). It appears, then, that the DoD has acknowledged that holding contractors completely liable for the unintentional inclusion of "counterfeits" may, in certain instances, be unfair.

It is ironic that this tacit acknowledgement is based on the long-standing practice of reimbursing contractors for nonconforming parts. Although the purchase and/or manufacture of nonconforming parts may be largely unavoidable, common sense dictates that remediation costs are the responsibility of the contractor who manufactured, oversaw the manufacture, or purchased the nonconforming parts. In the commercial sector, manufacturers regularly make decisions regarding nonconforming shipments, none of which entail additional payments from the customer. In fact, Howton (2012) asserted that by treating nonconforming parts as an inevitable part of doing business—versus a nuisance or distraction—manufacturers can realize significant savings by minimizing scrapped shipments. A firm's engineering team can quickly determine whether the nonconforming parts are still adequate or whether a simple design modification can be made. Often, delaying production is not cost effective if the risk is minimal.

With regard to actual counterfeit parts (i.e., fake parts or parts that have been intentionally manipulated by the source), the DoD must develop realistic policy that recognizes the difficulty and expense that contractors face in attempting to reduce the risk to zero, and the impact that this might have on overall system quality. Just as it is impractical to think that the commercial sector's quality control systems can eliminate nonconforming parts altogether, it is unrealistic to believe that prevention processes will eliminate the incidence of counterfeit parts in the DoD supply chain.

To be sure, nonconforming parts find their way into DoD systems more often that one might imagine, especially if rigorous quality control is lacking. In fact, one might argue that the high incidence of nonconforming parts in weapons systems is a consequence of the DoD's willingness to provide reimbursement. In its scathing review of the F-35 Joint Strike Fighter program, for instance, the DoD Inspector General (DoDIG; 2013) concluded that the program "did not sufficiently implement or flow down technical and quality management system requirements to prevent the fielding of nonconforming hardware and software" (p. i) The report included the following summary:

> We wrote 363 findings that identified a total of 719 issues for the six contractor assessments performed. There were multiple issues identified in most of the findings with

> [sic] the majority of issues were violations of the AS9100C Quality Management System standard. For each of the assessments, we classified the findings as major nonconformances, minor nonconformances, or opportunities for improvement (OFIs). Each finding received an additional technical review for accuracy and classification. (DoDIG, 2013, p. 6)

Regarding nonconforming parts and components, the DoDIG (2013) recorded numerous deficiencies, including the following:

- "airframes measured using the laser alignment system routinely did not meet mate and alignment drawing requirements" (p. 17);
- "Lockheed Martin personnel were using discrepant sealant mixing equipment for production" (p. 23);
- "composite cumulative adhesive shelf-life times were not recorded for some composite materials" (p. 23);
- "the liquid shim application process was not in compliance with documented procedures" (p. 23); and
- "drill bit life was not being tracked. Drill bit life should be tracked to ensure dimensional compliance" (p. 23).

In the case of the F-35, the failure to apply rigorous quality assurance has cost the DoD untold billions of dollars, which it will not recuperate given current policy. Holding contractors liable for parts and product nonconformance and improving contractor oversight through the hiring and training of an expanded government acquisition workforce will go a long way toward correcting deficient quality control systems. But holding contractors responsible for the inclusion of counterfeit parts that have been willfully and deceitfully manipulated, all while providing reimbursement for egregious manufacturing errors, represented a failure to properly order DoD priorities.

COUNTERFEIT GOODS – ELECTRONIC PARTS

With regard to any electronic parts procured by or on behalf of Seller for the Goods, Seller shall meet the following additional requirements:

i. Seller shall have a counterfeit electronic parts control plan that meets the intent of SAE standard AS5553A (Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition dated 2013-01).
ii. If Buyer or Seller suspects that Seller has procured counterfeit electronic parts, Seller shall quarantine such parts and make them available for investigation by appropriate U.S. Government authorities.
ii. Seller shall procure electronic parts from the Original Component Manufacturer (OCM) or its authorized (or franchised) distributor. In the event that Seller cannot procure electronic parts from the OCM or its authorized (or franchised) distributor, Seller shall obtain Buyer's written approval prior to procuring electronic parts from any party other than the OCM or its authorized (or franchised) distributors. With such request, Seller shall provide a plan for inspecting and testing such parts to ensure that they do not constitute Counterfeit Goods.
iii. Seller shall maintain all traceability and OCM-compliance documentation for electronic parts at its facility for seven (7) years from completion of this contract, or such other period as required elsewhere in this Contract, and make such documentation available to Buyer at its request.
iv. Seller shall include the substance of this article, including this flow down requirement, in all subcontracts awarded by Seller for work under this Contract.

Figure 13. Boeing's (2013) flowdown requirement for detection and prevention of counterfeit goods

Although the DFARS guidance is deficient in some respects, some of the criticism aimed at the supplement is clearly misguided. According to the supplement, firms that are not subject to cost accounting standards because of their smaller size are not required by law to establish and maintain a detection and prevention system. Representatives of large firms have taken aim at this exception, pointing out that because the vast majority of suppliers associated with the sale of suspect counterfeit parts are small, lower level sub-contractors, independent distributors, or brokers, the law should require that these entities maintain anti-counterfeit systems.

Livingston (2013) noted that prime contractors are "frequently systems architects and systems integrators who may not be involved in the direct procurement of electronic components; their lower tier suppliers tend to be in a more effective position to implement counterfeit electronic part avoidance and detection practices" (p. 2). Although this may be a true statement, it does not follow that these smaller entities should be legally required to implement an anti-counterfeit system. Prime and upper-tier contractors are responsible for the work of subcontractors, by definition. Indeed, one can argue that the prime contractor is in the "more effective position" to design, implement, and oversee the appropriate anti-counterfeit systems and ensure that the necessary components of these systems are flowed down appropriately. Large firms, it might be argued, were seeking a legal mandate in order to avoid the leg work of establishing flow-down requirements, monitoring subcontractors and suppliers, and ensuring compliance.

Large contractors can and should require their subcontractors and suppliers to take steps to avoid counterfeit parts and may go so far as to hold these lower-tier entities partially or fully liable for remediation in the event that counterfeit parts are discovered. Moreover, the flow down of anti-counterfeit measures is already a component of the SAE standards and is one of the elements of an adequate counterfeit detection system per Section 818. Figure 13 presents a list of flow-down requirements used by Boeing when hiring contractors.

Amendments to Section 818

It appears that Congress has come to realize that the incidence of counterfeit parts cannot be fully eliminated. Contractors, on occasion, must rely on suppliers other than OEMs. Moreover, the continued ambiguity surrounding the term "trusted supplier" is a further acknowledgement of how difficult it is to categorize sources. The critical nature of the component, differing calculations of risk versus benefit, and time sensitivity inform, to some extent, the level of "trust" assigned to a given supplier. Accordingly, Section 833 of the 2013 NDAA includes amendments to Section 818. The section was amended to read as follows:

> The cost of counterfeit electronic parts and suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are not allowable costs under Department contracts, unless—

> (i) the covered contractor has an operational system to detect and avoid counterfeit parts and suspect counterfeit electronic parts that has been reviewed and approved by the Department of Defense … (ii) the counterfeit electronic parts or suspect counterfeit electronic parts were provided to the contractor as Government property … and (iii) the covered contractor provides timely notice to the Government.

The amended version is an improvement over the original. However, the law remains deficient in some areas. Of greatest concern, there is still a lack of clarity with regard to what constitutes an adequate detection and prevention system. Additionally, some of Section 818's initial "actions following assessment" have not been fully addressed. For example, the DoD has yet to issue or revise remedial actions to be taken in the case of a supplier "who has repeatedly failed to detect and avoid counterfeit electronic parts."

VI. Recommendations & Conclusion

The threat of counterfeit parts within the DoD's supply chain is real. We can anticipate that that threat will only escalate over time—with potentially serious consequences. However, as previously stated, for the foreseeable future, the DoD can expect to continue to face budgetary challenges. Therefore, the DoD must be ever mindful of solutions that will have unacceptable budgetary impacts; it is critical that the DoD find an appropriate and acceptable balance between risks and costs.

Recommendations

This balance is reflected in the recommendations provided, which fall into three high-level categories: (1) strengthen standards, (2) implement stronger preventive measures, and (3) develop a long-term strategy.

Strengthen Standards

- **The DoD should require contractors to rely on recognized standards, such as SAE AS5553, in devising their counterfeit detection and mitigation procedures.**

  Currently, contractors cannot be sure that their detection and prevention systems will qualify for government approval. Moreover, there is no process to secure or document this approval. By requiring contractors to adhere to standards, there is less ambiguity, which makes it easier for contractors to design processes, and for the DoD to approve and verify these processes.

  Is should be noted that in the case of electronic parts, the requirements of standard AS5553 are "generic and intended to be applied or flowed down through the supply chain to all organizations that procure electronic parts and/or assemblies, regardless of type, size and product provided" (SAE, 2009, p. 3).

- **DoD program managers should partner with program contractors to determine an appropriate, individualized, risk-based approach to counterfeit mitigation that adheres to established standards.**

  Determining risk is a qualitative/quantitative process of combining three evaluated components, including threats (likelihood of occurrence), vulnerabilities (weaknesses or gaps in security from established standards, a measure of security effectiveness), and consequences (impact of adverse occurrences)

  This recommendation is in line with Standard AS5553, which states explicitly that "the mitigation of fraudulent/counterfeit Electrical, Electronic, and Electromechanical parts in this standard is risk-based and will vary depending on the desired performance or reliability of the equipment/hardware."

  With this in mind, the DoD should consider assigning weighted scores (similar to NASA) to contractors. The qualifying threshold could vary depending on the nature of the program and the specific priorities with regard to cost and risk.

- **The DoD should enforce quality assurance standards, recognizing that nonconforming parts threaten weapons system integrity and may lead to costly remediation.**

  The DoD often reimburses contractors for rework and corrective action in the case of nonconforming parts. Although the occasional purchase and/or manufacture of such parts may be largely unavoidable, common sense dictates that remediation costs are the responsibility of the contractor who manufactured, oversaw the manufacture, or purchased the nonconforming parts.

  The NDAA conflates the definitions of nonconforming parts and counterfeit parts. But a distinction must be drawn. The key difference is that the latter entails some form of willful deception on the part of the supplier that manipulates or manufactures the counterfeit item. Because the DoD often requires parts and components that are no longer

available through the OEM, upper-tier contractors turn to subcontractors, brokers, or other sources whose suppliers may engage in dishonest practices. Because subcontractors and brokers often rely on multiple suppliers to meet DoD demand, determining the provenance of counterfeits is exceedingly difficult, and given DoD budgetary constraints, it is unreasonable to anticipate the complete elimination of counterfeits from upper-tier contractors' supply chains. Simply, counterfeit elimination is unaffordable. Accordingly, it seems only fair that the cost of remediation be shared, provided that the contractor has in place a rigorous counterfeit detection and prevention system that is functioning properly.

Implement Stronger Preventive Measures

- **The DoD should, where appropriate, encourage the use of existing deterrents (e.g., tamper-proof packaging, x-ray inspection) while developing new anti-counterfeiting technologies.**

  The use of tamper-proof packaging, holograms, invisible printing, and so forth in the pharmaceutical industry has proven remarkably effective at reducing the incidence of counterfeit drugs in developed markets, particularly for high value and critical items. DoD suppliers could use tamper-proof packaging and other safeguards to transport items produced by OEMs and other trusted suppliers in addition to items that have been tested in order to ensure supply-chain integrity. These safeguards would protect sensitive electronic parts and components in two ways: they prevent the insertion of malicious functionality and guarantee the legitimacy of the part or component (through the use of unique packaging).

  At the same time, the DoD should encourage the development of universal standards with regard to track and trace technologies (e.g., plant DNA marking) by leveraging its buying power.

- **Debar suppliers who repeatedly furnish parts or components containing counterfeit parts.**

  As discussed, it is not the role of the DoD to supervise contractors' suppliers. Ideally, contractors' detection and prevention systems will deter "repeat offenders" from furnishing counterfeits. However, if a supplier continues to engage in practices—willfully, unintentionally, or as a consequence of indifference—that lead to the inclusion of counterfeit parts in DoD systems, the supplier should be barred from conducting business with the DoD and its contractors.

- **The DoD should require foreign companies to report suspect counterfeits using the GIDEP and provide penalties for non-compliance.**

  Currently, only U.S. and Canadian companies may participate in the GIDEP. However, suppliers and subcontractors from across the globe provide parts, components, and systems to the DoD. These parties should participate in reporting counterfeit and suspect counterfeit parts.

  It is therefore essential that the DoD and other government agencies work to ensure that the GIDEP is sufficiently robust to serve as the central mandatory reporting mechanism for counterfeit electronic parts.

Develop a Long-Term Strategy

- **The DoD should focus on best value, as opposed to lowest cost, in its acquisition of critical technologies.**

  The DoD has responded to recent budgetary pressures by increasing their reliance on lowest price technically acceptable (LPTA) criteria in assessing offerors' submissions. For any given solicitation, the decision to use the LPTA source selection process is identified in the request for proposals. The DoD is then bound to award the contract to

the vendor that offers the lowest evaluated price, provided that the proposal meets established technical threshold requirements.

Under LPTA, there is no need to perform trade-off analysis or to compare the specific technical solutions provided by multiple vendors. As a result, when using LPTA as the source selection criteria, there is a greater risk that the selected vendor may not provide the best-value service or product to the customer. Firms offering lower prices may have fewer, or less experienced, employees, unreliable supply chains, or less effective quality control processes—factors that may contribute to a higher incidence of counterfeits. Moreover, these factors are typically excluded from consideration under LPTA. The DoD should refrain from "buying cheap" for critical technologies because in the end, the long-term costs are often too high.

- **The DoD should minimize the impact of obsolescence by using (to the extent possible) parts and components for which multiple sources exist. Where this is not possible, the DoD must develop a robust obsolescence management strategy.**

  The DoD should require its contractors to mitigate the threat of parts obsolescence by relying on parts for which multiple, reputable, sources exists. In addition, contractors should be required to ensure that a common-build standard is maintained throughout each production run of a part or component in order to reduce the risk of obsolescence. These requirements should be built into the uniform standards for counterfeit detection and prevention issued by the DoD.

  In addition, parts used in design should be tracked for obsolescence issues throughout the system life cycle. This helps ensure the availability of parts by providing sufficient lead-time to develop the best resolutions to sustain fielded systems and reduce life-cycle costs. Many part-tracking databases are available to provide information concerning when a part is discontinued by its manufacturer.

- **The U.S. should strive to retain its design capabilities for critical technologies.**

  Globalization may lead to some loss of expertise in production of defense industrial goods. Over time, this could pose a significant problem. For instance, protectionists suggest that the DoD and American industry might be unable to judge the quality of foreign-produced goods, or that in the event of a global calamity, the United States might find it very difficult to move production back to the domestic industrial base. However, the solution to these problems is relatively straightforward: The United States must ensure that it retains the ability to design and produce critical technologies.

  Yet critics assert that America can only retain said capabilities by eschewing globalization and focusing on domestic design and production. This assertion relies on the observation that the emergence of truly transformative innovation seems to occur most readily within an environment that facilitates the gradual refinement of products. But this is largely the American paradigm. Although there is no doubt that it has led to great technical innovation, there are other models of success. In Japan, for example, transformative innovation is rare. Rather, Japan is well known for improving technologies that were initially designed in other countries. As a result, the Japanese consistently rank higher than the United States in technical industries such as electronics, automotive, and materials development. Clearly, then, there is no reason to think that the United States must maintain all of its current design and production capabilities in a particular field in order to integrate, and even improve, new technologies. In addition, more deliberative, global monitoring of new technologies, by both the DoD and industry, should allow the United States to keep pace with global innovation.

Conclusion

The threat of counterfeit parts within the DoD's supply chain is real and will only escalate over time, with potentially serious consequences. In order to reduce this threat,the DoD and its industry partners will have to work together to reduce the risk to acceptable levels, at an affordable cost. Although both parties may have the best intentions, it is essential that any incentives, penalties, and rewards are properly aligned in order to produce the desired outcome,

(i.e., without creating other unwanted consequences). The nation's military readiness depends on it.

References

AERI. (2014). Counterfeit electronic component detection. Retrieved from http://www.aeri.com/counterfeit-electronic-component-detection/

Aerospace AS5553 Resource Center. (2009). What is AS5553? Retrieved from http://www.as5553.com/

Aerospace Industries Association (AIA) of America, Inc. (2011). *Counterfeit parts: Increasing awareness and developing countermeasures.* Retrieved from http://www.aia-aerospace.org/assets/counterfeit-web11.pdf

Army Science Board (ASB). (2013). *The strategic direction for Army science and technology*. Retrieved from http://www.fas.org/irp/doddir/army/asb-strat.pdf

Barlas, S. (2008). California e-pedigree rules pose challenges for pharmacies. *Pharmacy & Therapeutics.* Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2683612/

Basel Action Network. (2007). Will Congress ban toxic e-waste trade? Retrieved from http://www.ban.org/2011/07/06/will-congress-ban-toxic-e-waste-trade/

Belva, M. (2010). *DoD should leverage ongoing initiatives in developing its program to mitigate the risk of counterfeit parts* (GAO-10-389). Washington, DC: Government Accountability Office.

Boeing. (2013). BDS terms and conditions. Retrieved from http://www.boeingsuppliers.com/idscommon/clauses/HXXX/H927_20131115.pdf

Brunello, B., & Robinson, C. (2011, October 18). *GSFC supplier assessments: Mitigating risks through corrective action* [Presentation slides]. Retrieved from http://supplychain.gsfc.nasa.gov/docs/sc2011b.brunelloc.robinsonasof1017.pdf

Capaccio, T. (2013). Pentagon using China satellite for U.S.-Africa Command. *Bloomberg News.* Retrieved from http://www.bloomberg.com/news/2013-04-29/pentagon-using-china-satellite-for-u-s-africa-command.html

Committee on Armed Services. (2012). *Inquiry into counterfeit electronic parts in the Department of Defense supply chain.* Washington, DC: Government Printing Office.

Congressional Budget Office (CBO). (2013). *Long-term implications of the 2013 Future Years Defense Program*. Retrieved from http://www.cbo.gov/sites/default/files/cbofiles/attachments/07-11-12 FYDP_forPosting_0.pdf

Defense Federal Acquisition Regulation Supplement (DFARS), 48 C.F.R. ch. 2 (2014).

Defense Logistics Agency (DLA) Land and Maritime. (2012). QSLD program Retrieved from http://www.landandmaritime.dla.mil/offices/sourcing_and_qualification/offices.aspx?section=QSL

Defense Science Board (DSB). (1999). *Final report of the Defense Science Board on globalization and security*. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology.

Defense Science Board (DSB). (2005). *High performance microchip supply*. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology.

Department of Defense Inspector General (DoDIG). (2013). *Quality assurance assessment of the F-35 Lightning II Program*. Washington, DC: Author.

Executive Office of the President of the United States. (2011). *2010 U.S. Intellectual Property Enforcement Coordinator Strategic Plan*. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_feb2011.pdf

Ferran, L. (2012, May 22). Counterfeit Chinese parts slipping into military aircraft: report. ABC News. Retrieved from http://abcnews.go.com/Blotter/counterfeit-chinese-parts-slipping-us-military-aircraft-senate/story?id=16403599

Fong, E. (2011, October 25). *Comprehensive program protection planning*. Presented at 14th Annual NDIA Systems Engineering Conference, San Diego, CA.

Forbes. (2013). The world's biggest public companies, aerospace & defense. Retrieved from http://www.forbes.com/global2000/list/#page:1_sort:0_direction:asc_search:_filter:Aerospace%20%26%20Defense_filter:All%20countries_filter:All%20states

Foster, S. (2012). *Dryden Flight Research Center* [Presentation slides]. Presented at Dryden Flight Research Center. Retrieved from http://www.erai.com/presentations/General%20Session%201/NASA-Steve%20Foster.pdf

Freedberg, S. (2012, October). DLA demands chip makers tag products with plant DNA: A war on counterfeiters. *Breaking Defense*. Retrieved from http://breakingdefense.com/2012/10/dla-demands-chip-makers-tag-products-with-plant-dna-a-war-on-co/

Garamone, J. (2012, May 23). DoD combats counterfeit parts threat. *American Forces Press Services*. Retrieved from http://www.defense.gov/News/NewsArticle.aspx?ID=116456

GlaxoSmithKline. (2011). Government affairs, public policy and patient advocacy. Retrieved from http://www.gsk.com/content/dam/gsk/globals/documents/pdf/GSK-on-counterfeiting-of-healthcare-products.pdf

Government Accountability Office (GAO). (2010). *Defense supplier base: DOD should leverage ongoing initiatives in developing its program to mitigate risk of counterfeit parts* (GAO-10-389). Washington, DC: Author.

Government Accountability Office (GAO). (2012). *DoD supply chain: Suspect counterfeit electronic parts can be found on internet purchasing platforms* (GAO-12-375). Washington, DC: Author.

Grow, B., Chi-Chu, T., Edwards, C., & Burnsed, B. (2008). Dangerous fakes. *Bloomberg Businessweek.* Retrieved from http://www.businessweek.com/stories/2008-10-01/dangerous-fakes

Hamermesh, D. (2013). When demand elicits fake supply. Retrieved from http://freakonomics.com/2014/01/27/when-demand-elicits-fake-supply/

Howton, J. (2012). To scrap or not to scrap. Retrieved from http://www.manufacturing.net/articles/2012/08/to-scrap-or-not-to-scrap

ISPE: International Leadership Forum. (2010). *Supply chain security: A comprehensive and practical approach*. Tampa, FL: Author.

Johnson, N. B. (2012a). Feds, industry split over counterfeit parts strategy. *Federal Times.* Retrieved from http://www.federaltimes.com/article/20121126/DEPARTMENTS01/311260007/ Feds-industry- split-over-counterfeit-parts-strategy

Johnson, N. B. (2012b). How NASA fights counterfeiting. *Federal Times*. Retrieved from http://www.federaltimes.com/article/20121130/DEPARTMENTS01/311300005/How-NASA-fights-counterfeiting

Kim, S. (2012). Hundreds of exploding fake Heinz bottles discovered in New Jersey. *ABC News*. Retrieved from http://abcnews.go.com/Business/hundreds-counterfeit-heinz-ketchup-bottles-discovered-jersey/story?id=17511614

Knock offs catch on: Fake goods are proliferating to the dismay of companies and governments. (2010, March 4). *The Economist*. Retrieved from http://www.economist.com/node/15610089

Lechleiter, J. (2012, August 22). Exposing and eradicating the dark world of fake pharmaceuticals. Retrieved from http://www.forbes.com/sites/johnlechleiter/2012/08/22/exposing-and-eradicating-the-dark-world-of-fake-pharmaceuticals/

Livingston, H. (2010). *Securing the DOD supply chain from the risks of counterfeit electronic components: Recommendations on policies and implementation strategy*. Retrieved from http://counterfeitparts.files.wordpress.com/2012/02/securing_the_dod_supply_chain_from_the_risks_of_counterfeit_electronic_components.pdf

Livingston, H. (2013). *An assessment of the proposed DFARS rule on detection and avoidance of counterfeit electronic parts*. Retrieved from http://counterfeitparts.files.wordpress.com/2013/06/assessment_re_proposed_dfars_rule_case2012-d055_1306083.pdf

McKinney, D. (2001, August). *Impact of commercial off-the-shelf (COTS) software and technology on systems engineering* [Presentation slides]. Retrieved from http://www.incose.org/northstar/2001Slides/McKinney%20Charts.pdf

Metzger, R. (2013). DoD counterfeit parts rule: So little after so long. Retrieved from http://www.law360.com/articles/447201/dod-counterfeit-parts-rule-so-little-after-so-long

Moran, T. (1990). The globalization of America's defense industries. *International Security, 15*(1), 57–99.

National Aeronautics and Space Administration (NASA). (2013). *NASA parts policy* (NASA Policy Directive NPD8730.2C). Retrieved from http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=8730&s=2C

National Aeronautics and Space Administration (NASA) Authorization Act of 2010, Pub. L. No. 111-267, § #, 124 Stat. 2805 (2010).

National Defense Authorization Act (NDAA) for Fiscal Year 2012, Pub. L. No. 112-81, § 818, 125 Stat. 1298 (2011).

National Defense Authorization Act (NDAA) for Fiscal Year 2013, Pub. L. No. 112-239, § 833, # Stat. # (2012).

Oberhettinger, D. (2008). Counteracting the threat of counterfeit components. Retrieved from http://www.nasa.gov/offices/oce/llis/imported_content/lesson_1832.html

OECD. (2011). The economic impact of counterfeiting and piracy. Retrieved from http://www.oecd.org/fr/sti/ind/theeconomicimpactofcounterfeitingandpiracy.htm

Office of Management and Budget (OMB). (2012). *Budget of the United States Government, Fiscal year 2013: Analytical perspectives*. Washington, DC: Author.

Peters, P. (2012, June 6). *Anti-counterfeit.* Presentation at the Product Support Manager Conference by Deputy Assistant Secretary of Defense Supply Chain Integration, Fort Belvoir, VA.

Pfizer. (2013). Counterfeiting and importation. Retrieved from http://www.pfizer.com/products/counterfeit_and_importation/counterfeit_importation?qt-counterfeiting_importation=2#7

President's Blue Ribbon Commission on Defense Management. (1986). *Final report to the president.* Washington, DC: Author.

Root, J. (2011). *GSFC supplier assessments* [Presentation slides]. Safety and Mission Assurance Directorate, Goddard Space Flight Center. Retrieved from http://supplychain.gsfc.nasa.gov/docs/sc2011j.rootasof1020.ppt.pdf

SAE International. (2013). Aerospace Standard 5553: Fraudulent/counterfeit electronic parts; avoidance, detection, mitigation, and disposition. Retrieved from

http://standards.sae.org/as5553a/Sivcovich, K. (2012). *NASA supplier assessment experience* [Presentation slides]. DRS Sensors & Targeting Systems. Retrieved from http://supplychain.gsfc.nasa.gov/docs/SC2010-K.Sivcovich.pdf

Trent, R., & Roberts, L. (2010). Managing global supply and risk. Fort Lauderdale, FL: J. Ross.

United States Department of Commerce. (2010). *Defense industrial base assessment: Counterfeit electronics.* Washington, DC: Bureau of Industry and Security, Office of Technology Evaluation. Villasenor, J. (2013). *Compromised by design? Securing the defense electronics supply chain*. Retrieved from http://www.brookings.edu/~/media/research/files/papers/2013/11/4%20securing%20electronics%20supply%20chain%20against%20intentionally%20compromised%20hardware%20villasenor/villasenor_hw_security_nov7.pdf

Winter, C. (2013, August 14) How the Pentagon is using DNA to combat counterfeiters. *Bloomberg.* Retrieved from http://www.businessweek.com/articles/2013-08-14/how-the-pentagon-is-using-dna-to-combat-counterfeiters

World Health Organization (WHO). (2013). General information on counterfeit medicines. Retrieved from http://www.who.int/medicines/services/counterfeit/overview/en/

Zulueta, P. (2011, June 29). *Counterfeit electronics: NASA update* [Presentation slides]. NASA Jet Propulsion Laboratory and California Institute of Technology. Retrieved from http://nepp.nasa.gov/workshops/etw2012/submissions/talks/Wednesday/1130%20-%20Counterfeit%20Electronics%20-%20NASA%20Update.pdf

Zulueta, P. (2012, May 17). *Industry game changers: SAE G-19 standards updates*. Retrieved from http://www.erai.com/presentations/General%20Session%201/Industry%20Game%20Changes%20-%20Phil%20Zulueta.pdf

Acknowledgements

This research was sponsored by the Naval Postgraduate School, and we are especially grateful for the support and encouragement provided by Rear Admiral Jim Greene (USN Ret.) and Keith Snider. We would also like to acknowledge Jinee Burdg, a graduate student at the University of Maryland's School of Public Policy, whose research contributed to this report. Finally, we would like to thank our co-worker Caroline Dawn Pulliam for her assistance with the planning and coordination of this study.

About the Authors

Jacques S. Gansler

The Honorable Jacques S. Gansler, former under secretary of defense for acquisition, technology, and logistics, is a professor and holds the Roger C. Lipitz Chair in Public Policy and Private Enterprise in the School of Public Policy, University of Maryland; he is also the director of the Center for Public Policy and Private Enterprise. As the third-ranking civilian at the Pentagon from 1997–2001, Dr. Gansler was responsible for all research and development, acquisition reform, logistics, advance technology, environmental security, defense industry, and numerous other security programs. Before joining the Clinton Administration, Dr. Gansler held a variety of positions in government and the private sector, including deputy assistant secretary of defense (material acquisition), assistant director of defense research and engineering (electronics), senior vice president at TASC, vice president of ITT, and engineering and management positions with Singer and Raytheon Corporations.

Throughout his career, Dr. Gansler has written, published, testified, and taught on subjects related to his work. He is the author of five books and over 100 articles. His most recent book is *Democracy's Arsenal: Creating a 21st Century Defense Industry* (MIT Press, 2011).

In 2007, Dr. Gansler served as the chair of the secretary of the Army's Commission on Contracting and Program Management for Army Expeditionary Forces. He is a member of the Defense Science Board and the Government Accountability Office (GAO) Advisory Board. He is also a member of the National Academy of Engineering and a fellow of the National Academy of Public Administration. Additionally, he is the Glenn L. Martin Institute Fellow of Engineering at the A. James Clarke School of Engineering; an affiliate faculty member at the Robert H. Smith School of Business; and a senior fellow at the James MacGregor Burns Academy of Leadership (all at the University of Maryland). From 2003–2004, he served as interim dean of the School of Public Policy at the University of Maryland and from 2004–2006, Dr. Gansler served as the vice president for research at the University of Maryland.

William Lucyshyn

William Lucyshyn is the director of research and a senior research scholar at the Center for Public Policy and Private Enterprise in the School of Public Policy at the University of Maryland. In this position, he directs research on critical policy issues related to the increasingly complex problems associated with improving public-sector management and operations and with how government works with private enterprise.

His current projects include modernizing government supply-chain management, identifying government sourcing and acquisition best practices, and analyzing Department of Defense business modernization and transformation. Previously, Mr. Lucyshyn served as a program manager and the principal technical advisor to the director of the Defense Advanced Research Projects Agency (DARPA) on the identification, selection, research, development, and prototype production of advanced technology projects.

Prior to joining DARPA, Mr. Lucyshyn completed a 25-year career in the U.S. Air Force. Mr. Lucyshyn received his bachelor's degree in engineering science from the City University of New York and earned his master's degree in nuclear engineering from the Air Force Institute of Technology. He has authored numerous reports, book chapters, and journal articles.

John Rigilano

John Rigilano is a faculty research assistant at the Center for Public Policy and Private Enterprise. He earned his Master of Public Policy degree from the University of Maryland, College Park in 2011, and holds a Bachelor of Arts degree in anthropology from the Pennsylvania State University. He is pursuing a career in policy and program analysis.

The Center for Public Policy and Private Enterprise provides the strategic linkage between the public and private sector to develop and improve solutions to increasingly complex problems associated with the delivery of public services — a responsibility increasingly shared by both sectors. Operating at the nexus of public and private interests, the Center researches, develops, and promotes best practices; develops policy recommendations; and strives to influence senior decision-makers toward improved government and industry results. The Center for Public Policy and Private Enterprise is a research Center within the University of Maryland's School of Public Policy.