

Defense Standardization Program Journal

October/December 2013

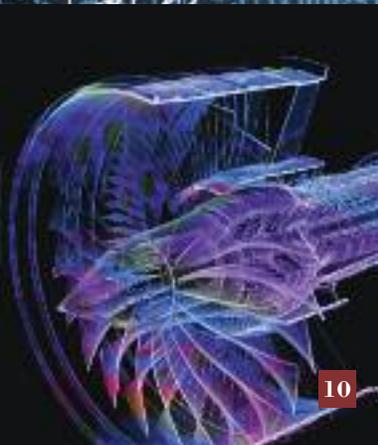


Counterfeits

Deterrence in Depth
GIDEP Helps Mitigate the Risk of Counterfeits
Combating Counterfeits
Contractor Anticounterfeit Programs
Proven Standards



3



10



28

1 Director's Forum

3 Deterrence in Depth

One Stakeholder's View of DLA and the Counterfeit Electronics Invasion

10 GIDEP Helps Mitigate the Risk of Counterfeits

17 Combating Counterfeits

Knowing Your Supply Chain

21 Contractor Anticounterfeit Programs

Opportunities for Improvement

28 Proven Standards

A Product of Technical Excellence

Departments

38 Program News 45 Events 46 People

The *DSP Journal* is available only in electronic form.

To receive issues, please subscribe at the DSP website, www.dsp.dla.mil,
or e-mail DSP-Editor@DLA.mil and put "Subscribe" in the subject line.

The *Defense Standardization Program Journal* (ISSN 0897-0245) is published four times a year by the Defense Standardization Program Office (DSPO). Opinions represented here are those of the authors and may not represent official policy of the U.S. Department of Defense. Letters, articles, news items, photographs, and other submissions for the *DSP Journal* are welcomed and encouraged. Send all materials to Editor, *DSP Journal*, Defense Standardization Program Office, 8725 John J. Kingman Road, STOP 5100, Fort Belvoir, VA 22060-6220. DSPO is not responsible for unsolicited materials. Materials can be submitted digitally by the following means:

e-mail to DSP-Editor@dlm.mil
CD or DVD to *DSP Journal* at the above address.

DSPO reserves the right to modify or reject any submission as deemed appropriate.

Gregory E. Saunders

Director, Defense Standardization Program Office

Tim Koczanski

Editor, Defense Standardization Program Journal

Defense Standardization Program Office

8725 John J. Kingman Road, STOP 5100

Fort Belvoir, VA 22060-6220

703-767-6888

Fax 703-767-6876

dsp.dla.mil



Director's Forum

“A Little Bit Of This, A Little Bit Of That” or “It Takes A Whole Village”— How We Plan to Defeat the Plague of Counterfeit Parts

This title may sound a bit like a “Rocky and Bullwinkle” episode featuring Boris and Natasha, but like Boris and Natasha, the bad guys are sometimes unsophisticated and the plot fails through dumb luck. Sometimes the plot fails because everyone contributed a little bit, just enough, and often it is because every member of the village did their level best. As you will see in this issue of the *DSP Journal*, the solution to our counterfeit challenge is similarly a team effort and lies in the right mix of policy, regulations, technical analysis, logistics procedures, criminal prosecution, and more, by organizations from the Secretary of Defense (or Energy, Transportation, Justice, etc.) down to the suppliers of piece parts.

In 2012, Congress directed the Department of Defense to establish a plan to detect and avoid the counterfeit electronics that have been entering our supply chain. This edition offers a snapshot of many of the aspects of the solution.

The battle against counterfeits and counterfeiting takes a multi-pronged approach that can be compared to a military campaign. Everyone knows his or her part and everyone must be ready to adapt. Just as the criminals adapt to our countermeasures, we adapt as our systems age, applying new practices based on the realities of the sustainment phase. Diminished manufacturing sources and shortages of materiel to support our weapon systems lead to vulnerabilities. If you can no longer procure from the original manufacturer because the product was discontinued, you have to search the “gray market” where things are not always as they appear.

While counterfeit jeans, purses, and CDs pose risks to our economic system, counterfeit electronics and other products on which we rely present a danger to public health and safety in general: citizens, first responders, warfighters, and critical infrastructure are all vulnerable to counterfeits.



Gregory E. Saunders
Director
Defense Standardization Program Office

In this issue of the *Journal*, we slice the problem in several planes.

DLA examines the challenge from the perspective of the basic building blocks—the piece parts procured to support our troops.

GIDEP shows how sharing knowledge can help the larger team effort. As the community discovers better and better fakes, we must continue to share what we find so others can be on the lookout.

The DLA supply chain article by Harry Frost looks at ways to maintain long-term adequate supply that we can trust.

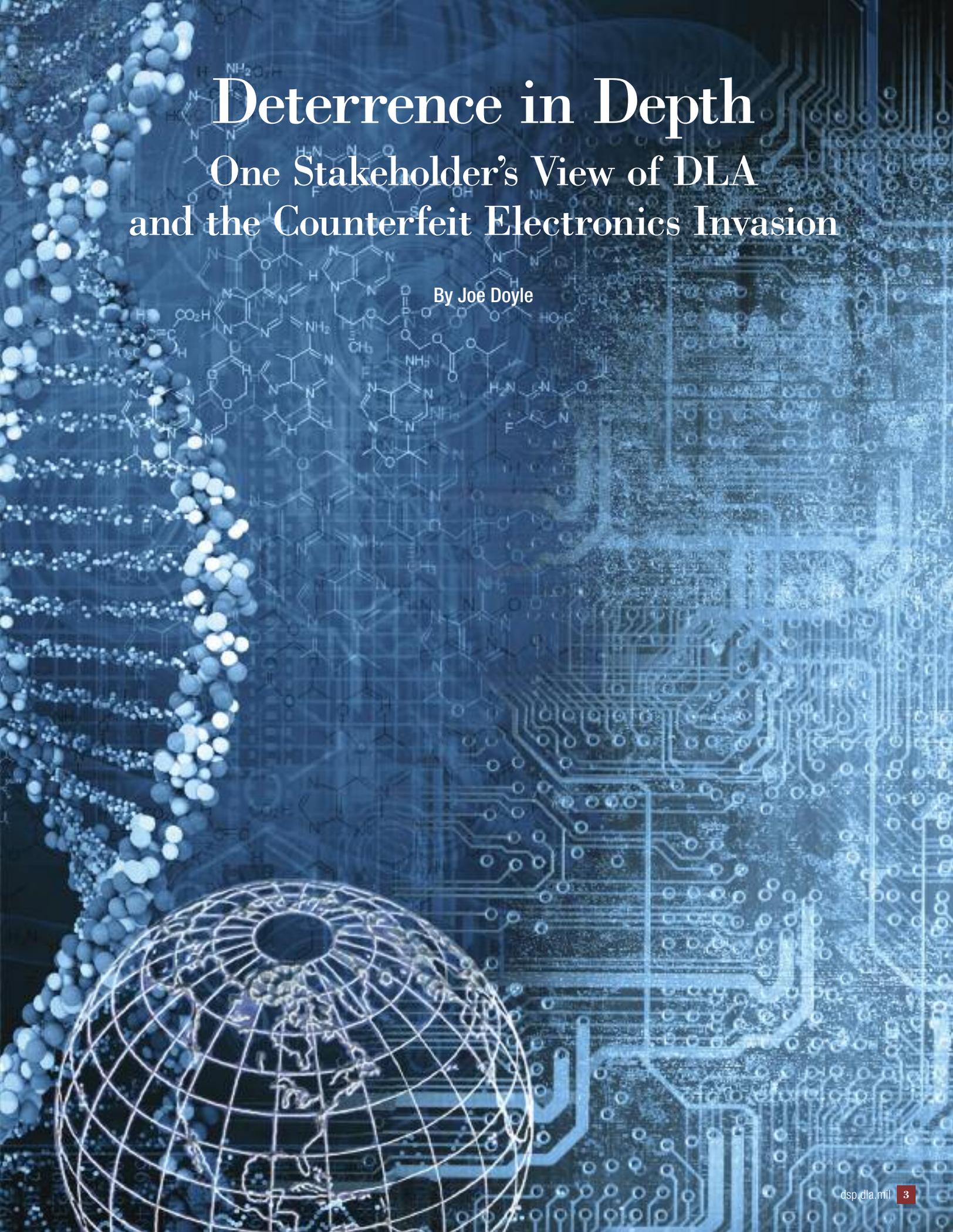
In the article from the Missile Defense Agency, you will read how government agencies are prototyping policies and regulations most appropriate to their sectors.

Through our partnership with industry, we are teaming with private-sector standards developers in a robust effort to create broadly accepted standards to combat counterfeiting. These standards help combine the many ideas that the government and industry teams have been forging over the last few years.

When you get right down to it, counterfeiting is deception perpetrated by criminals. And sometimes, when the criminals succeed in getting counterfeits into the supply chain, even trusted sources can unintentionally become pawns in their deadly game. To combat it, we all will have to exercise great vigilance because we all have something to lose. The United Nations estimates that counterfeiting is third behind illicit drugs and human trafficking in serious international criminal activity. In one edition of the *Journal*, we can't examine the breadth of counterfeiting, but the articles and many of the strategies and tactics are equally relevant to other major categories of counterfeiting—consumer goods, pharmaceuticals, machine parts, and dozens of other products. One thing we've learned is that almost no product is too small or too cheap, nor too expensive or too complicated, to attract increasingly sophisticated counterfeiters.

Unfortunately, in the technical and logistics pursuits of ways to combat counterfeiting in the federal supply chain, we face an adversary that is always adapting—almost like a virus. We are used to dealing with the laws of physics (or chemistry or biology), which do not often change. In those fields, when we succeed we can put a plaque on the wall—polio eradicated, food production rate quadrupled, or automotive vehicle safety drastically improved—because our achievements are durable. Unfortunately, fighting counterfeiting requires technical solutions that are nearly ephemeral. They last only until our adversary finds a way to counteract our measures and discovers a better means to disguise the counterfeits. So, we have to be agile, continuing to refine our battle plans. An admiral, speaking at a conference I attended, noted, “There are no permanent victories. To win is to stay alert and maneuver.” No saying better typifies our challenges in dealing with counterfeits and counterfeiters.

These articles represent a snapshot, not a final plan, of how the federal-industrial base is approaching the problem of counterfeit parts in our supply chain.



Deterrence in Depth

One Stakeholder's View of DLA and the Counterfeit Electronics Invasion

By Joe Doyle

The Defense Logistics Agency (DLA) is the nation's combat support agent for logistics. DLA obtains and supplies almost 100 percent of the consumable items for America's warfighters. The agency manages over 5.1 million parts, supports more than 2,500 weapon systems, and accounts for nearly 85 percent of the spare parts for our military forces. The intricate supply chains for these commodities are truly global in nature.

DLA adopts a threefold approach in executing its combat support role. The agency's three focus areas are (1) warfighter support, (2) stewardship excellence, and (3) workforce development. Although these three work in harmony, DLA's director, Vice Admiral Mark D. Harnitchek, makes it clear that "DLA's top priority is always warfighter support."¹ The introduction of counterfeit electronic products in the military supply chains poses a significant threat to our nation's warfighters and the weapon systems on which they depend. DLA's nearly 27,000 women and men are committed to deterring the threat posed by this counterfeit electronics invasion.

The Counterfeit Electronics Invasion

Historically, we most often used the word "invasion" when referring to a military force assaulting a foe's territory. The term takes on a broader meaning in modern usage. Merriam-Webster lists one definition as "the incoming or spread of something usually hurtful."² Likewise, TheFreeDictionary defines the word as "a large-scale onset of something injurious or harmful."³ It is not an exaggeration to apply the term to the infiltration of global supply chains by counterfeit electronics.

In 2011, the Senate Armed Services Committee conducted a series of hearings into the threat of counterfeit electronic parts in the DoD supply chains.⁴ The threats are real and come from both international and domestic sources. These hearings and subsequent investigations have confirmed the growing threat that counterfeit parts—including electronics—pose to our Air Force, Army, Navy, and Marine Corps personnel.

In response to this growing realization, Section 818 of the National Defense Authorization Act (NDAA) of 2012 directed "an assessment of Department of Defense acquisition policies and systems for the detection and avoidance of counterfeit electronic parts." Congress reinforced its concern in Sections 807, 833, and 1603 of the 2013 NDAA.

The invasion of counterfeit electronics is not isolated; rather, it occurs over a wide front. These incursions continue to expand and increasingly threaten all sectors of society. In an August 28, 2013, blog, Andrew Olney, chair of the Semiconductor Industry Association (SIA) Anti-Counterfeiting Task Force, stated that "counterfeit chips can end up in a wide range of critical consumer, industrial, medical, and military applications, posing a clear and immediate threat to public health and safety."⁵

Technology is improving at an increasingly rapid pace. This brings about many beneficial capability advancements for most users. DoD prefers to take full advantage of technology improvements. However, budgetary and other constraints demand extending the useful service life of many weapon systems beyond that envisioned during their development. In a paper on Diminishing Manufacturing Sources and Material Shortages, Henry Livingston—the technical director at BAE Systems Electronic Systems and an influential spokesperson on counterfeit electronic parts—reminds us that “the manufacturing lives of many critical items get shorter while the life cycles of military weapon systems keep increasing.”⁶ Unfortunately, this creates additional pressures for DLA and its supply chain partners in supporting aging weapon systems with products that original manufacturers may no longer be producing.

In October 2013, DLA Land and Maritime hosted the 2013 Electrical and Electronics Industry Outreach Forum. Industry and government stakeholders devoted much of that forum to the growing danger posed by counterfeit electronics. Two observations framed the discussion:

- Counterfeit electronics pose “a growing risk to mission readiness, personnel safety and national security.”⁷
- “Electrical & Electronic Components ranked 1 of top 5 five commodities most vulnerable to counterfeits.”⁸

The DLA Defense

DLA’s logistics role across the military services creates a complex environment for the deterrence of counterfeit electronics. Well before the legislative mandates, DLA embarked on a proactive approach to assessing and addressing supply chain risks. The agency collaborates with industry to develop recommended approaches and solution sets. DLA’s Combating Counterfeiting Program is one case in point. DLA initiated a series of layered measures to detect and deter counterfeit products across its supply chains. The agency directs many of its efforts at electrical and electronic components, because they ranked highest of the commodities deemed most vulnerable to counterfeits.

Warriors during the centuries of the Iron Age and Middle Ages often relied on chain mail (interlocking metal rings) to protect them from pointed and bladed threats (arrows, knives, pikes, and so on) of their day. Counterfeit electronic parts pose an equally deadly threat to 21st century warfighters. I liken DLA’s multidimensional approach to a chain mail of “Ts”—training, threat assessments, trusted sources, traceability, testing, and technology—that protect the DLA supply chains from unwanted penetration and thus help defend against the electronics counterfeit invasion.

Training

DLA provides both operational and technical training to its workforce. In addition, the agency developed and initiated counterfeit awareness training across the enterprise. This training is mandatory for most of DLA's 27,000 employees, including those in management, procurement, receiving, and testing positions. Annual refresher training helps ensure that DLA personnel stay attuned to the constantly evolving threat environment that counterfeit electronic products pose.

Threat Assessments

Electronics counterfeiters are an inventive and profit-driven lot. They persistently come up with new ways of infiltrating once-safe supply chains. Among its research and development (R&D) efforts, DLA fosters and deploys a range of threat assessments to inform its risk management strategies. These assessments are broad based and do not focus solely on identified high-risk commodities. The agency also engages a variety of human intelligence and technology-enabled assessments of product providers and their supply chain partners.

Trusted Sources

DLA is committed to buying electronics from demonstrated trustworthy sources whenever possible. The agency screens, qualifies, and compiles lists of those reliable sources of supply. In the microcircuit and semiconductor arenas, for example, DLA Land and Maritime specifies trusted sources in qualified manufacturers lists (QMLs), qualified products lists (QPLs), and qualified suppliers lists for distributors, among others. DLA continues to refine its controls, including establishing qualification lists for other electronics and non-electronic products.

Traceability

Whenever possible, DLA requires that electronics suppliers provide item traceability back to the original manufacturer. Requirements in purchase orders and long-term contracts provide that the contractor furnish DLA with a certification of traceability initiated by the electronic item manufacturer:

To ensure this conformance, the contractor must provide a Certificate of Conformance and Traceability (CoC/T) with the information and documentation required by the applicable military specification. This documentation must reference the contract number and include a certification signed by the approved QPL/QML manufacturer. In addition, if the material is not procured directly from the approved manufacturer, all additional documentation required by the specification must be provided to establish traceability from the QPL/QML manufacturer through delivery to the Government.⁹

DLA frequently reviews its procedures and tightens controls on electronic component traceability processes across supply classes.

Testing

The agency periodically strengthens its product testing and product verification programs. DLA scrutinizes new sources, products that are exceptionally vulnerable, and areas of greatest potential profit for counterfeiters. The agency conducts increased testing of those commodities deemed at high risk of counterfeiting. This testing comprises inspection and acceptance testing at point of origin, production lot testing during manufacturing, and random product quality inspections throughout the item life cycle. When testing uncovers electronics counterfeits, DLA invokes specific quarantine and disposal procedures. These measures help ensure that confiscated counterfeit items do not escape into the global e-waste environment only to surface later to threaten supply chains.

Technology

Industry is producing some very promising risk identification, anticounterfeiting, and authentication technologies. Through its Weapon System Sustainment Program, DLA conducts R&D to uncover and tailor those emerging technologies best suited to its battle against counterfeits. Supplier risk assessments include such items as database mining and business intelligence efforts. Certain anticounterfeiting methods include overt features (holograms, item unique identification, serialization, and so on), while others rely on covert methods such as hidden images and watermarks. In the case of electronic parts, authentication technologies play an increasingly critical role. DLA's DNA marking requirement is a prime example. DLA requires that suppliers of electronic microcircuits (Federal Supply Class 5962) mark each item with a botanically based SigNature® DNA marker. Depending on a variety of factors, these covert marks either distinguish an authentic microcircuit or establish provenance of the item to the trusted source. Supply chain personnel can rapidly identify those DNA-marked items in the field. They can also send them to DLA's Electronic Product Test Center for screening and further routing to the laboratory for definitive forensic analysis.

The Rest of the Story

We can more accurately compare the electronics counterfeit story to a literary series as opposed to a single novel. Electronics counterfeiters are shrewd. Counterfeiting techniques in the microcircuit and semiconductor arenas continue to evolve. Counterfeit electronics providers routinely change part markings to disguise obsolete lot codes or misrepresent commercial products as high-reliability military grade. Unscrupulous suppliers refurbish used devices and sell them as new. Earlier electronics counterfeiters used relatively primitive sanding, blacktopping, and re-marking tactics. Those have now

morphed into such sophisticated counterfeiting techniques as flat lapping, micro blasting, and laser etching.

Industry and government segments continue to collaborate in developing improved barriers to help thwart electronics counterfeiters. The Government-Industry Data Exchange Program provides one way for the sectors to share information. The federal regulations mentioned earlier are gradually leading to new, stronger inspection practices and purchasing procedures. High-intensity magnification and surface texture inspection are becoming more commonplace. Anticounterfeiting standards are becoming more widespread.

SAE International established the G-19 Counterfeit Electronic Parts Committee “to develop standards suitable for use in aeronautic, space, defense, civil and commercial electronic equipment applications to mitigate the risks of counterfeit electronic components.”¹⁰ SAE issued standard AS5553, “Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition,” in April 2009 and issued the revised AS5553A in January 2013. AS5553 applies to manufacturers. Individual manufacturers are adding increased layers of brand, product, and trademark protection. A companion SAE standard, AS6081, encompasses distribution. “This standard provides uniform requirements, practices, and methods to mitigate the risks of purchasing and supplying fraudulent or counterfeit electronic parts for distributors.”¹¹ The critical need to ensure quality products has given rise to an entire industry focused on authentication methods and anticounterfeiting technologies.

The conflict between those who traffic in counterfeit electronics and those who require authentic products will escalate. The counterfeit electronics invasion will continue, and DLA’s deterrence in depth is one defense. I would have preferred to conclude this view by borrowing broadcaster Paul Harvey’s famous closing tag line: “And now you know the rest of the story.” Unfortunately, the saga of DLA’s battle with counterfeit electronics is far from over, and another stakeholder will have to chronicle the rest of the story.

¹Vice Admiral Mark D. Harnitchek, “DLA Director’s Focus Areas,” http://www.dla.mil/pages/areas_focus.aspx, October 2013.

²Merriam-Webster, <http://www.merriam-webster.com/dictionary/invasion>, November 2013.

³TheFreeDictionary by Farlex, <http://www.thefreedictionary.com/invasion>, November 2013.

⁴Carl Levin, Chairman, Senate Armed Services Committee, “Opening Statement at SASC Hearing on Counterfeit Electronic Parts in DoD Supply Chain,” November 8, 2011, <http://www.levin.senate.gov/newsroom/speeches/speech/opening-statement-at-sasc-hearing-on-counterfeit-electronic-parts-in-dod-supply-chain>.

⁵Andrew Olney, Chairman, Semiconductor Industry Association Anti-Counterfeiting Task Force, “SIA’s New Anti-Counterfeiting Whitepaper: A Roadmap in the Battle Against Counterfeit Semiconductors,” August 28, 2013, <http://www.semiconductors.org/blog>.

⁶Henry Livingston, Vice-Chair, Government Electronics and Information Technology Association, G-12 Solid State Devices Committee, *Diminishing Manufacturing Sources and Material Shortages (DMSMS) Management Practices*, http://www.dmea.osd.mil/docs/geb1_paper.pdf.

⁷“Counterfeit Prevention Team Supply Chain Risk Management Logistics Operations (J3),” *2013 Electrical and Electronics Industry Outreach Forum*, Columbus, OH, <http://www.landandmaritime.dla.mil/downloads/news/ElectricalElectronics.pdf>.

⁸Ibid.

⁹*DSCC Master Solicitation for Automated Solicitations and Resulting Awards*, Revision 21, June 2006, http://docsfiles.com/pdf_dscs_master_solicitation_for_automated_solicitations_and_awards.html.

¹⁰SAE International, G-19 Counterfeit Electronic Components Committee, Committee Charter, November 2007.

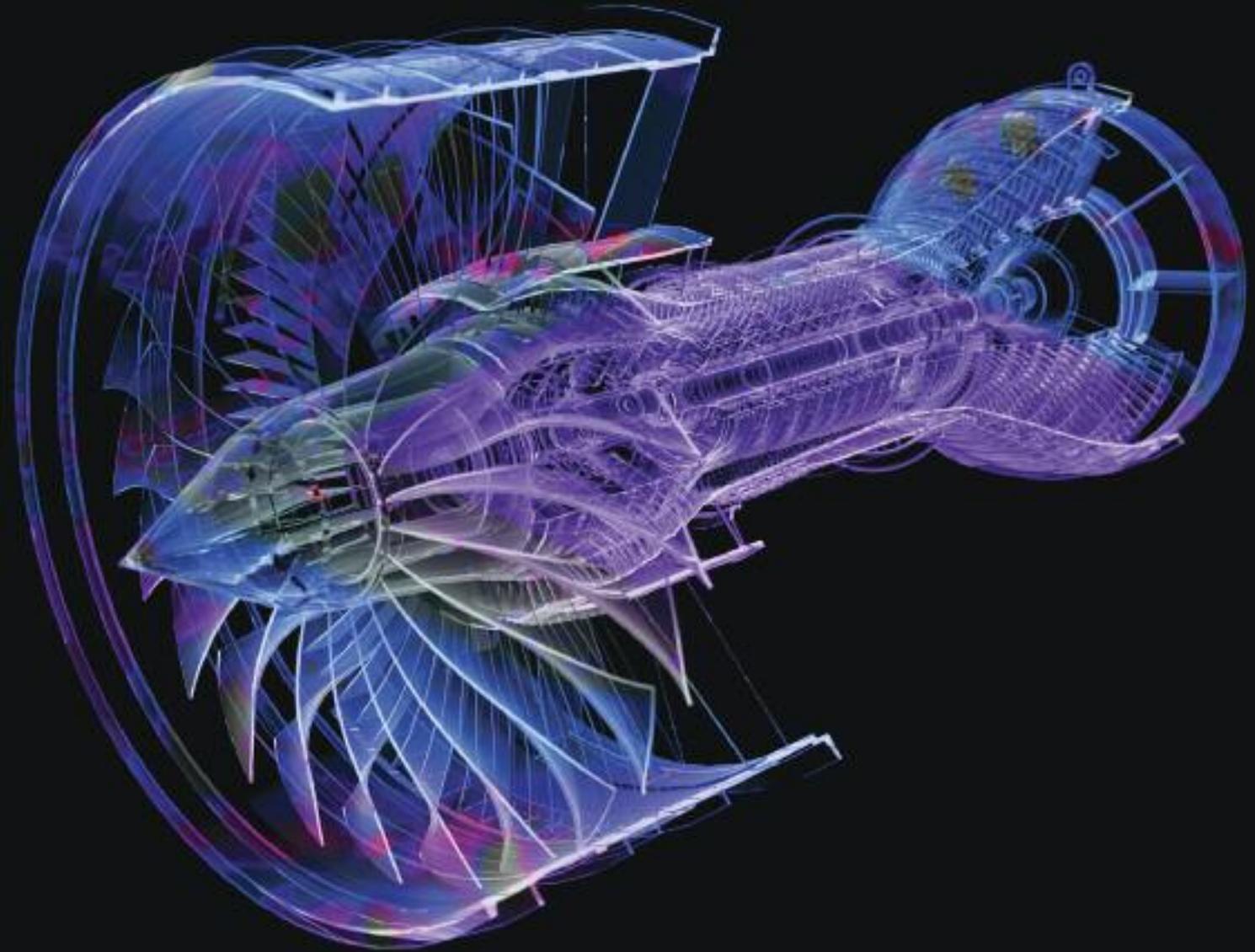
¹¹Matthew R. Shindell, Todd Kramer, and Stanley H. Salot Jr., “The ‘Ticking Time Bomb’ of Counterfeit Electronic Parts,” *Industry Week*, July 22, 2013, <http://www.industryweek.com>.

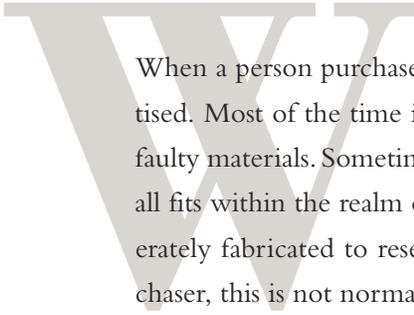
About the Author

Joe Doyle is a retired submarine officer and a senior consultant at LMI. He manages a variety of R&D initiatives for DLA's Weapon System Sustainment Program and similar tasks for other federal agencies. Dr. Doyle actively participates across academic, government, and industry anticounterfeiting efforts. He is a certified Project Management Professional and Certified Manager. Dr. Doyle teaches management and other business disciplines at both the undergraduate and graduate levels. ✨

GIDEP Helps Mitigate the Risk of Counterfeits

By Bill Pumford and Rudy Brillon





When a person purchases a product, he or she expects the product to function as advertised. Most of the time it does, but sometimes it does not. Sometimes it fails because of faulty materials. Sometimes it fails due to poor workmanship. Sometimes it just fails. This all fits within the realm of normal experience. However, when a bogus product is deliberately fabricated to resemble the genuine product with the intent to deceive the purchaser, this is not normal. This is counterfeit.

Counterfeit parts and materials are a major issue faced by DoD today. This issue is not new, but it is becoming more and more prevalent and cannot be allowed to go unchecked. The Government-Industry Data Exchange Program (GIDEP) has a major role in mitigating this issue.

Counterfeits—The Issue

In 2007, the Naval Air Systems Command (NAVAIR) asked the Department of Commerce (DOC) to conduct a defense industrial base assessment of counterfeit electronics. This request was motivated by NAVAIR's suspicion of an increasing number of counterfeit electronics infiltrating the DoD supply chain.

In January 2010, DOC published its findings in *Defense Industrial Base Assessment: Counterfeit Electronics*. On the basis of interviews with major segments of the U.S. supply chain, DOC found that “39 percent of companies and organizations participating in the survey encountered counterfeit electronics” and that there had been “an increasing number of counterfeit incidents being detected, rising from 3,868 in 2005 to 9,356 incidents in 2008.” The report goes on to provide general findings and recommendations on how the U.S. Government could “inhibit the circulation of counterfeit electronics.” Two of those recommendations are (1) “report all suspect and confirmed counterfeit components to federal authorities and industry associations” and (2) “consider establishing a centralized federal reporting mechanism for collecting information on suspected/confirmed counterfeit parts for use by industry and all federal agencies.”¹

In March 2010, the Senate Armed Services Committee (SASC) announced its investigation into the issue of counterfeit parts in the DoD supply chain. Following the conclusion of its investigation, the SASC conducted a hearing on November 8, 2011, to refine its understanding of the findings. One finding, germane to this discussion, was the following:

Another place where the defense industry is coming up short is in reporting cases of counterfeit parts. Our investigation uncovered approximately 1,800 cases where parts suspected to be counterfeits have been identified by companies in the defense supply chain. However, the vast majority of those cases appear to have gone unreported to the Department of Defense or criminal authorities. In addition, too few

contractors and distributors consistently file reports with the Government-Industry Data Exchange Program (GIDEP). ...That has to change. Failing to report suspect counterfeits and suspect suppliers puts everyone at risk. We need to make sure our regulations require contractors who discover suspected counterfeit parts in a military system to report that discovery to the military right away. We should also require DoD and contractors to report cases of suspected counterfeits found in the supply chain into GIDEP, so that others are alerted.²

To address that finding, the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112-81) mandated that the Secretary of Defense “conduct an assessment of Department of Defense acquisition policies and systems for the detection and avoidance of counterfeit electronic parts” and, with regard to the reporting of suspect counterfeits, 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).

As part of its response, DoD, in April 2013, published DoD Instruction 4140.67, “DoD Counterfeit Prevention Policy,” which included the following direction regarding the reporting of counterfeits: “Document all occurrences of suspect and confirmed counterfeit materiel in the appropriate reporting systems including the Government-Industry Data Exchange Program (GIDEP).”

About GIDEP

GIDEP began in 1959 as the Inter-service Data Exchange Program (IDEP). IDEP was created by mutual agreement of the Army, Navy, and Air Force in an effort to reduce duplicate qualification and environmental testing being conducted for the military services by various contractors on the same parts, components, and materials. At its inception, IDEP covered only the ballistic missile effort of the U.S. defense programs.

Shortly after its establishment, IDEP began a collaboration with industry. As the information needs of the U.S. defense industries changed, IDEP was expanded to include other types of data and information.

During this period, the Navy initiated the Components Reliability History Survey (CRHS) program, designed to exchange documented test and related information on high-reliability parts and components used in the military’s various ballistic missile programs. The Navy also had a parallel effort—the Guided Missile Data Exchange Program

(GMDEP)—to collect reliability information for its guided missile programs. GMDEP was designed to exchange reliability and test information on parts and components used in the Navy’s other missile programs. The Navy’s CRHS program and GMDEP were merged into IDEP in 1963 and 1964, respectively.

In 1965, the National Aeronautics and Space Administration (NASA) asked to join IDEP to improve the exchange of data related to parts used in space applications. Upon joining IDEP, NASA began issuing “alerts” on parts, components, and materials that did not meet specifications for space requirements. As a result, many IDEP participants began exchanging “alert” information on nonconforming parts and components used by the military and NASA.

As a result, many IDEP participants began exchanging “alert” information on nonconforming parts and components used by the military and NASA.

During this same time, the Canadian Military Electronics Standards Agency (CAMESA), part of the Canadian Department of National Defence, requested permission to join IDEP to exchange data among Canadian industry and government activities and their U.S. suppliers. The Canadian Government and the U.S. Department of State signed a memorandum of agreement in 1966, and the Canadian Department of National Defence became a member and sponsor of IDEP. As a result of NASA and CAMESA joining IDEP, the program’s name was changed to the Interagency Data Exchange Program. At the same time, the scope of the data for IDEP was changed to accept test and reliability data on all missile and aerospace programs.

In 1970, the three military services’ IDEP offices were consolidated by agreement of the Joint Logistics Commanders (JLCs), and the program was renamed the Government-Industry Data Exchange Program. By request of the JLC, the Navy assumed overall management of GIDEP.

In 1980, as the importance of energy and energy exploration increased, the Department of Energy (DOE) joined GIDEP, and selected DOE data were added to the program. DOE data in GIDEP have since expanded to cover the areas of development and

production of parts, materials, components, and related energy subjects for solar, wind, fossil fuel, oil, and nuclear energy.

In 1991, the Office and Management Budget issued Policy Letter 91-3, "Reporting Nonconforming Products," designating GIDEP as the central database for government-wide reporting of nonconforming products and materials. In 1995, DoD designated GIDEP as the central repository for Diminishing Manufacturing Sources and Material Shortages (DMSMS) obsolescence information.

In 2007, GIDEP was moved from the Assistant Secretary of the Navy for Research, Development and Acquisition to DSPO.

Today, GIDEP is a DoD program promoting and facilitating the sharing of technical information among government agencies and industry partners to increase system safety, reliability, and readiness and to reduce system development, production, and ownership costs. Through its web-accessible database containing failure experience, product information, metrology, engineering, and reliability/maintainability data, GIDEP supports a membership of 335 government agencies and 2,055 industry companies from the United States and Canada.

How GIDEP Helps Mitigate the Risk of Counterfeits Today

As identified in the DOC assessment and the SASC investigation, one of the essential components to mitigating the risk of counterfeits is the collection and sharing, by government and industry, of information on suspect counterfeits. GIDEP has a long and successful history of facilitating the exchange of information between these two groups. GIDEP has also been the focal point for establishing a government and industry-wide network of experienced professionals wrestling with parts and materiel management issues in the DoD supply chain.

Reporting suspect counterfeits through GIDEP is not something new; one of the earliest suspect counterfeit reports dates back to 1968. The GIDEP Industry Advisory Group surveyed the GIDEP membership in 1977 to assess the extent and impact of counterfeit electronic parts at that time. More than 200 members responded to the survey, with 43 reporting that they had discovered counterfeit parts; the respondents also shared their recommended courses of action.³ Since then, the GIDEP community has submitted reports on suspect counterfeits of a wide range of parts and materials, including both electronic and nonelectronic items. Today, as it did back then, GIDEP provides a vehicle for reporting all the necessary information to help identify and disposition suspect counterfeit parts and materials.

When it receives a suspect counterfeit report, GIDEP reviews it to ensure it is fact based and verifies that the referenced supplier has had an opportunity to provide input. Once this is completed, GIDEP processes the report and enters it into the GIDEP database. Through weekly or customized notices, the members of the GIDEP community are alerted about the availability and applicability of the report so that they can retrieve the information and take whatever action may be appropriate.

Another aspect of GIDEP that helps in mitigating the risks of counterfeits is its repository of DMSMS data. Obsolete parts, or parts nearing obsolescence, are prime candidates for counterfeiting. By utilizing the obsolescence information in the GIDEP database, a member can monitor the health of its parts and proactively reduce the counterfeit risks.

GIDEP can share only the information that is reported to it. However, even though the program, processes, and system are in place to meet the challenge, GIDEP is not being fully utilized. Many more instances of counterfeits are occurring than are being reported. That is about to change.

How GIDEP Can Help Mitigate the Risk of Counterfeits Tomorrow

Through the years, GIDEP has transformed itself to better meet its mission by revising its policies and by taking advantage of new technology, enabling the program to move from hard-copy documents to the World Wide Web. With the growing attention and importance of the counterfeit issue, the number of GIDEP users and suspect counterfeit reports being submitted is expected to grow significantly. At the same time, the globalization of the marketplace has opened up new partnerships that will need to be accommodated. Close coordination with international allies and the international supply chain will create new vistas for information sharing. GIDEP is working, and will continue to work, closely with the appropriate communities to ensure that any changes to GIDEP will address their needs and concerns. In response to these new requirements, GIDEP will modernize its policies, business processes, and information systems to meet the needs of its users.

You Can Help GIDEP Mitigate the Risk of Counterfeits

Join GIDEP and become a member of the team. Membership is free. Simply access <http://www.gidep.org/join/requirements.htm> and submit your application today.

By becoming a member, you will become part of the community that is tackling this critical issue. By submitting your data, others will benefit from your experiences, and by

downloading their data, you will benefit from theirs. It is this interactive sharing of information by people like you that will enable GIDEP to help mitigate the risk of counterfeits.

¹Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, *Defense Industrial Base Assessment: Counterfeit Electronics*, January 2010.

²Carl Levin, Chairman, Senate Armed Services Committee, “Opening Statement at SASC Hearing on Counterfeit Electronic Parts in DoD Supply Chain,” November 8, 2011, <http://www.levin.senate.gov/newsroom/speeches/speech/opening-statement-at-sasc-hearing-on-counterfeit-electronic-parts-in-dod-supply-chain>.

³Department of Defense, Government Industry Data Exchange Program, *Final Report of GIDEP Industry Advisory Group Survey of Counterfeiting of Electronic Parts*, H. D. Hoyt Jr., GIDEP Index Number 347.20.00.00-S3-18, Document Number S3-MR-77-01, June 1977.

About the Authors

Bill Pumford and Rudy Brillon work at the GIDEP Operations Center.

Mr. Pumford is the subject matter expert on suspect counterfeit reporting and is the lead technical consultant to the GIDEP Program Office. With 20 years of program experience, Mr. Pumford also manages the Operations Center’s DMSMS program, with responsibility for overseeing the collection and dissemination of discontinued product information to the GIDEP community.

Mr. Brillon, the Operations Center’s director, has spent the last 28 years developing, implementing, operating, and maintaining information systems in support of DoD maintenance, configuration, logistics, ordnance, and metrology management programs.✱

Combating Counterfeits

Knowing Your Supply Chain

By Harry Frost



Is knowing your supply chain the same as the “old boys’ club”? Definitions, connotations, and semantics all play a role in answering that question. Combating counterfeit hardware, such as nuts, bolts, or screws, is similar to, but in many ways different than, combating counterfeit designer clothing, jewelry, CDs, prescription drugs, or electronics. Each industry must assess its needs and potential vulnerabilities with respect to the counterfeit issue. The intent of this article is to provide some insight into the qualified suppliers list (QSL) program used by Defense Logistics Agency (DLA) Troop Support’s industrial hardware supply chain and to show that the QSL program is an important contributor to the fight against counterfeit material.

DLA Troop Support’s QSL program encompasses the QSL for manufacturers and the QSL for distributors. The program satisfies one of the most highly identified, if not the most important, tenet of combating counterfeits: know and work with your supplier base—both manufacturers and distributors. So how does the old boys’ club reference fit in? We want to write to the suppliers and have them write to us. We want to e-mail them and have them e-mail in return. We want to talk with them and establish a rapport. And we want to visit with them. We want to know how they operate, and we want to be able to work out solutions while remaining confident that both parties are treated fairly and appropriately.

But does this mean that the supply chain is unfairly restrictive or provides some manner of favoritism or benefit, notions that are often used to characterize an old boys’ club? The answer to that question is an unequivocal “no.” The QSL program is *not* an old boy’s club.

DLA Troop Support’s QSL program is open to any applicant that can demonstrate compliance with criteria and provisions. Further, continued participation naturally requires continued compliance.

This qualification program encompasses the best industry practices and incorporates these elements into the DLA Troop Support Construction & Equipment (C&E) & Industrial Hardware Organization’s acquisition process. Under the program, we pre-qualify manufacturers and/or distributors to supply certain items based on an assessment of the provider’s applied process controls. Applicants must demonstrate that the controls which they have in-place and in-use on a daily basis comply with the established QSL Criteria, providing maximum assurance that the products procured conform to specification and contractual requirements.¹

For a subset of competitively procured items, suppliers are required to participate in the QSL program in order to sell those items to DLA. A qualified manufacturer can sell them directly to DLA. A qualified distributor can sell material that was produced by a qualified QSL manufacturer. Naturally, distributors must maintain accurate records to

demonstrate traceability directly to that manufacturer. They can even sell to DLA if they can demonstrate traceability through any qualified QSL distributor, as long as the item was manufactured by a qualified QSL manufacturer. This is referred to as “closed loop traceability.” Under no circumstances can distributors in the QSL program alter or modify the hardware in any way.

Six distinct commodity areas have QSL requirements. Table 1 lists them and shows the number of items, qualified manufacturers, and qualified distributors.

Table 1. Commodity Areas with QSL Requirements

Commodity area	Description
Class 3 threaded fasteners ^a	46,321 items 146 qualified manufacturers 113 qualified distributors
Class 2 threaded fasteners ^a	22,580 items 142 qualified manufacturers 109 qualified distributors
Rivets: blind aerospace and threaded pin rivets	5,824 items 23 qualified manufacturers 73 qualified distributors
Quick release pins	2,594 items 5 qualified manufacturers 43 qualified distributors
Rope: fiber rope, cordage, twine, and tape	415 items 20 qualified manufacturers 7 qualified distributors
Bulk metals	14,327 items 172 qualified distributors

^aThe class number refers to the class of thread fit.

Although the requirements for the commodity types have many similarities, each commodity type has its own tailored criteria and provisions. As an example, consider the quick release pin. Most people would recognize that these types of pins are used in exercise equipment. Weight lifting machines found at fitness centers use quick release pins to select a desired weight. However, many of these types of pins are used in more demanding applications, such as aircraft wing folds, ejection seat safety locks, ground vehicles, and ground support equipment tow attachments. Such applications require pins that have more robust performance. The industry standards that define the technical characteristics (shear strength, corrosion resistance, operability, resistance to sand and dust) have qualification test requirements. Therefore, the QSL program for quick release pins is

different than that for the other QSL commodities in that it has requirements for the review of each manufacturer's qualification test reports prior to their inclusion in the program.

The QSL program criteria address such topics as management responsibility, document control, purchasing, product traceability, lot control and marking, inspection of material, test control, test and measurement equipment, procedures for handling nonconforming material and corrective actions, packaging, training, records control, and audits (internal and external). Requirements to manage these areas are not unique to the QSL program. Examination of similar quality control systems defined by most consensus industry standards organizations reveals that controls in these same areas are required.

Not all industries face the same problems with counterfeits. Knowing our supply chain is a huge step in reducing the threat in the fastener arena, but there is no silver bullet to solve all problems. For example, the designer apparel industry has a "knowing" market for counterfeit garments, though not right, proper, or legal. Those interested in the counterfeit item are interested in the "look" only, at a deeply discounted price, of course. They would have no concern about the quality of a garment, the quality of a high-end watch (for example, whether it is actually waterproof to 2 atmospheres), or the wrong they are committing by purchasing the counterfeit. This same circumstance does not occur in the fastener community.

The QSL program at DLA Troop Support is not unique to DoD. The manufacturers and distributors that supply DLA also support the commercial aerospace, ground vehicle, and maritime community. And original equipment manufacturers (OEMs) in those industries institute their own quality programs for suppliers. The fact that our qualified suppliers have business relationships with OEMs in the non-DoD sector is a good thing. It demonstrates that the supplier (manufacturer or distributor) is in it for the long term; they are "on the grid," so to speak. And ultimately, that's what we want. To avoid standard counterfeit material, we want know "who we're dealing with."

¹See <http://www.troopsupport.dla.mil/Hardware/Technical/qsl.asp>.

About the Author

Harry Foster is a supervisory mechanical engineer at DLA Troop Support, Philadelphia, PA. 

Contractor Anticounterfeit Programs

Opportunities for Improvement

By Fred Schipp

Counterfeit electronic parts have become increasingly visible as a significant concern for hardware. In late 2011, a Senate hearing on the infiltration of counterfeit electronic parts into DoD systems provided a wake-up call to DoD and defense contractors alike. The main points disclosed by the hearing were as follows:

- Counterfeit electronic parts can be easily found whenever parts cannot be bought from authorized suppliers.
- The majority of counterfeit electronic parts originate in China.
- Buying from U.S.-based suppliers does not provide confidence that the parts are authentic or that they did not originate overseas.
- Many defense contractors are not sufficiently addressing the counterfeit part risk, specifically, through containment and reporting of counterfeit electronic parts.

The hearing led to the inclusion of Section 818, “Detection and Avoidance of Counterfeit Electronic Parts,” in the National Defense Authorization Act for 2012. That, in turn, led to the release of DoD Instruction 4140.67, “DoD Counterfeit Prevention Policy,” in April 2013.

The Missile Defense Agency (MDA) has been actively seeking to reduce or eliminate the counterfeit parts risk since 2006. The agency’s actions have included the development of rigorous requirements for the avoidance, detection, containment, and reporting of counterfeit parts and material, as well as assessments and audits of contractors and unauthorized suppliers of electronic parts.

One of MDA’s biggest challenges is to ensure an adequate flow-down of counterfeit part requirements through the entire ballistic missile defense program. The challenge is due to the program’s complex, layered network of sensors and interceptors and a command and control structure designed to enable quick response to an incoming missile threat with the appropriate interceptor types. That difficulty is exacerbated by the large number of contractor facilities—more than 1,000—that purchase, produce, or use electronic parts for their portion of an overall MDA system. Some of the contractors are six levels or more removed from the MDA program office.

Because of concerns with the difficulty of flowing requirements six levels or more into its supply chain, MDA developed a detailed assessment checklist in early 2012 to assist with audits of the contractor supply chain. The checklist has some 50 questions that, together, address all major aspects of counterfeit parts. The questions are grouped into nine sections: supplier selection; obsolescence management; handling, storage, traceability, and analysis; containment; subcontractor flow-down verification; detection; reporting; supplier assessment; and training.

The questions are ratable, with guidance provided for scoring. The rating system was intentionally developed to make it difficult to get a perfect score. In other words, a top rating of “5” for a response to a question indicates that the contractor not only met MDA’s requirements, but also met MDA’s “wish list” for the best possible compliance system. Here’s an example: MDA requires contractors to buy from authorized suppliers whenever possible. However, the agency does not control how the contractor meets that requirement. In this case, a “perfect” system would have two separate approved supplier lists (one for authorized and another for unauthorized suppliers) and an electronic purchasing system that does not allow unauthorized supplier purchases without documented management approval. The terms “authorized,” “unauthorized,” and “approved” suppliers are defined as follows:

- *Authorized supplier.* The supplier has been contractually authorized by the component manufacturer to market its product. Franchised distributors and component manufacturers are authorized suppliers.
- *Unauthorized supplier.* The supplier is not an authorized supplier. Independent distributors and brokers are unauthorized suppliers.
- *Approved supplier.* The contractor has reviewed the supplier and found it to be an acceptable source of parts. An approved supplier may be either authorized or unauthorized.

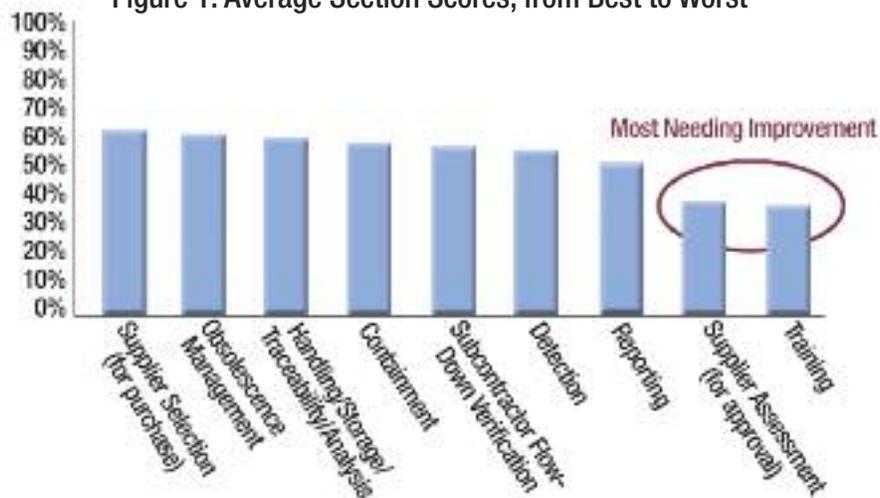
In addition to establishing a system for rating responses to the questions, MDA assigned a significance factor to each question. For example, the agency considers the question “Does the purchasing process require selection of parts from authorized suppliers as the first priority?” to be more significant than the question “Does the process for adding suppliers include verification of ISO 9001 and/or AS9120 certification?” The overall score of the contractor gives higher weighting to the questions of higher significance.

To date, MDA has audited seven contractor facilities and believes the sample size is sufficient to provide some guidance for other DoD organizations and their contractor supply chains. Figure 1 shows the average scores by checklist section, from best to worst. As the figure shows, training and supplier assessment are most in need of improvement. In both cases, the agency found the contractors, on average, to be less than 40 percent compliant with a “perfect” system. Two points about the findings are particularly pertinent:

- The audited contractors were primarily tier 2 or 3 contractors, generally with 100 to 500 employees at that location.
- Some confusion may exist about the difference between supplier assessment and supplier selection. Supplier assessment is the contractor’s process for determining which suppliers are least risky for providing counterfeit parts; that process builds the approved

supplier list. Supplier selection is the contractor's process for picking the lowest-risk supplier when it is time to buy parts.

Figure 1. Average Section Scores, from Best to Worst



Training

Much of the defense contractor supply chain is populated with small companies. Tier 3 or lower contractors may have fewer than 100 employees. They produce a specific assembly type for which they have expertise. Companies of this size usually have little capability to develop a solid training program. Travel funding for conferences is limited, and employees are less likely to have dedicated job titles. Further, although some companies had started training programs, the programs were focused primarily on awareness. In short, it was apparent that the training was not adequate to educate all affected parties. Furthermore, the cost for each contractor to develop its own training program would likely be passed on to MDA through increased assembly pricing, potentially adding substantially to the agency's costs.

To address the lack of adequate training, MDA used internal resources to develop a training program intended to be provided to all of its contractors. The training covers awareness, DoD requirements, MDA requirements, supplier assessment and purchasing recommendations, examples of counterfeit parts, and other information. The agency released this training in November 2013 to its prime contractors for release as necessary throughout the MDA contractor supply chain.

Supplier Assessment

MDA found supplier assessment to be inadequate for several reasons. Small contractors are more likely to "buy local," with the use of these suppliers deemed less risky. Although most contractors appear to have a form for assessing suppliers, the form often only confirms certification to a quality management system, points of contact, financial informa-

tion, and verification of compliance to the contractor's contract clauses. We found one supplier assessment form that overall was very good. However, the entire extent of the counterfeit assessment portion was this question: "Do you have a counterfeit parts avoidance process in place compliant with AS5553?" The expected answer is "yes," but unless the assessment team is properly trained, it will not be able to verify that answer.

Below are several other observations regarding assessments of suppliers in the defense supply chain that are less than optimal, along with recommendations for improvement:

- *Verification of the supplier's assessment process.* Approved suppliers should prove that they maintain robust processes for selecting low-risk sources for the parts they sell. A good system should have a multilevel approval process, with tiers to quantify the risk, and it should include a promise to buy from those low-risk suppliers first.
- *Use of government data.* If possible, contractors should use government systems, such as the System for Award Management or the Government-Industry Data Exchange Program (GIDEP), to obtain important information such as the supplier's history and current problems.
- *Proper handling of parts.* Although not specifically a counterfeit parts concern, some contractors do not confirm that their suppliers can be trusted to handle products in compliance with industry standards, such as the American National Standards Institute's (ANSI's) "Electrostatic Discharge Control Program Standard" (ANSI/ESD S20.20) or the joint IPC/JEDEC "Standard for Handling, Packing, Shipping, and Use of Moisture/Reflow Sensitive Surface-Mount Devices" (J-STD-033).
- *Inspection and testing of electronic parts.* Some contractors place too much trust in their suppliers. Specific inspection and testing requirements should be spelled out for all parts bought from unauthorized suppliers. MDA's *Parts, Materials, and Process Mission Assurance Plan* contains a table listing the required inspections and tests. The Society of Automotive Engineers (SAE) standard AS6081, "Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition—Distributors," also lists recommended inspections and tests. Contractors should not expect suppliers to know what tests to perform or to perform them.

Other Opportunities for Improvement

Responses to several other questions in the MDA checklist indicate additional opportunities for improvement:

- *Do test failure analysis processes include consideration of whether parts were bought from unauthorized sources?* Figure 2 shows MDA's rating guidance for the questions, allowing scores from 0 to 5. In this case, the average score was 0. No one could show proof that if assembly-level test failures are traced to an electronic part, the part is checked to de-

termine if it was bought from an unauthorized supplier (high risk). This is a critical issue, because without an awareness of counterfeit parts, it is possible (perhaps likely) that assembly-level test failures will not be checked for the potential of being counterfeited. This may result in a failure to contain installed counterfeit parts.

- *Is there a percent defective allowable (PDA) specified when parts are bought from unauthorized sources, which precludes the screening and use of parts that exceed the defect limit?* This is another important point, for which our “5” rating is summarized as follows: “Documented process requires a full analysis for all lots with a failure rate over 2%, including authorized suppliers. Parts must be contained pending results. Customer is notified for input.” We have seen recent information suggesting that a 2 percent defect rate is too low and that a defect rate of 5 percent is more reasonable. This is due to a failure rate on older (obsolete) products that may approach 5 percent even on authentic parts, due to oxidation, handling, etc. Regardless, it is important not to assume that electrically screening out failures on parts bought from unauthorized suppliers will always result in reliable parts.

Figure 2. Rating Guidance
Biggest Challenges to Compliance

Checklist Question	Section	C%	Best Practice (Rated 5 of 5)
Do test failure analysis processes include consideration of whether parts were bought from unauthorized sources?	Handle	0%	Documented process requires all failures to be checked for supplier type. If the supplier was unauthorized, process requires authenticity analysis.

Contractor—the audited company

Supplier—the contractor’s potential distributor supplier

Guidance for each rating score (0 through 5)	0	Failures are not checked back to supplier type (authorized vs unauthorized).
	1 (20%)	Excessive test fallout (>10%) will result in a check for supplier type. The contractor will consult his customer for guidance.
	2 (40%)	Excessive test fallout (>10%) will result in a check for supplier type. If the supplier was unauthorized, process requires authenticity analysis. No documented process.
	3 (60%)	All multiple failures must be checked for supplier type. If the supplier was unauthorized, process requires authenticity analysis. No documented process.
	4 (80%)	Documented process requires all multiple failures to be checked for supplier type. If the supplier was unauthorized, process requires authenticity analysis.
	5 (100%)	Documented process requires all failures to be checked for supplier type. If the supplier was unauthorized, process requires authenticity analysis.

■ *Does the purchasing process check GIDEP information for risky part numbers and suppliers?*

MDA has found that most contractors check GIDEP alerts for the potential that the reported part number may affect their own hardware. Specifically, contractors verify that those parts were not bought from the reported supplier and, in most cases, find no connection. However, few contractors also check the reported supplier against their own approved supplier list. It is MDA's position that suppliers that ship counterfeit parts (and that are subsequently reported to GIDEP) should be considered high-risk suppliers. Those suppliers should not be present on a contractor's approved supplier list unless or until the contractor has been able to assess and affirm that corrective actions are in place to once again consider the supplier a low-risk option.

Summary

A robust anticounterfeit program is not something that can be created quickly and easily. A truly comprehensive program must consider all aspects of the process, including assessment, purchasing, inspection, installation, failure analysis, containment, and reporting. In addition, DoD organizations must assist with developing a robust program. This may include audits or streamlining of their response procedures when a contractor requests assistance or reports an issue. DoD and defense contractors must work together for the best possible solution to this serious problem.

About the Author

Fred Schipp has supported MDA's Quality and Safety organization in all aspects of counterfeit parts policy since 2006, including the development of DoD and industry documents and standards for counterfeit electronic parts. He has helped MDA remain on the leading edge of counterfeit avoidance by participating in many assessments and audits of defense contractors and unauthorized suppliers, and in 2011, he assisted Senate Armed Services Committee staff members in the investigation of counterfeit electronic parts. Mr. Schipp works at the Naval Surface Warfare Center in Crane, IN. ✨

Technical excellence drives the development of uniformity of practices that results in standards that can be applied throughout an organization, reducing costs and mitigating risk. Initiatives that address the enhancement of an organization's technical excellence are key to the organization's maintaining a high level of performance on current programs and projects, as well as to its preparing for new programs and projects. This article addresses the interrelationship of standards and technical excellence, and it discusses some related National Aeronautics and Space Administration (NASA) initiatives, of which good standards are an important part.

Technical Excellence

Technical excellence is the goal of all organizations and individuals, whether in government or industry, national or international. What do we mean by technical excellence? Most people have their own ideas and interpretation as to what constitutes technical excellence. Entering "technical excellence" into the search page of Google produces a significant number of results, evidence that technical excellence is important to a large number of organizations and people, whether in the engineering discipline or other disciplines.

According to "Mr. Webster," excellence is defined as the state, quality, or condition of excelling; superiority. To excel is to be better than, or to surpass, others. We believe most, if not all, people would be comfortable with this definition. However, because the intent of this paper is to demonstrate the importance of technical excellence relative to proven standards, it may be appropriate to explore some statements that have been made concerning technical excellence.

One author defined technical excellence as an effort to ensure that well-considered and sufficient technical thoroughness and rigor are applied to programs and projects under an uncompromising commitment to safety and mission success.¹

Another author identified four guiding principles to achieving technical excellence:²

- Clearly documented proven policies and procedures
- Effective training and development
- Engineering excellence
- Continuous communications.

The same author also stated that two fundamental attributes must be considered when pursuing technical excellence: (1) personal accountability, whereby each individual must understand and believe that he or she is responsible for the success of the organization's mission, and (2) organizational responsibility, whereby the organization provides the proper training, tools, and environment.³

It has also been noted that, due to the rapidly expanding technology and science, engineers and technologists in the 21st century must have a strong technical background in their fields and understand technology at the interface between traditional fields.⁴ They must be creative, skilled problem solvers who can think critically using sound principles and concepts. Technical excellence and good standards are products of these principles.

Louis Armstrong is understood to have remarked that if you have to ask what jazz is, you will never know. (His exact words are not known, but it is accepted that he said something to this effect.) This remark could also apply to technical excellence. This becomes clear when one tries to quantify the meaning of technical excellence by producing metrics to establish whether a particular objective or goal has been achieved. For example, what provides a measure of the technical excellence achieved by an organization: number of patents received? number of professional journal publications? number of individuals with advanced degrees? number of engineers versus nonengineers at work? positive versus negative feedback on products? equipment or system successes versus failures? profit a company makes? number of standards it uses?

In the aerospace arena, one can certainly equate organizational technical excellence—and thus proven engineering and use of technically proven standards—to mission success. In the final analysis, technical excellence is one of the most important goals of any organization. How one achieves and maintains it is another question for which there is no simple answer. Unquestionably, an organization with recognized technical leaders who have vision, superior technical competence, and the desire to excel will achieve technical excellence. Development of proven standards is certainly a product of this goal. Thus, technical leadership is key for an organization's success and the ability of the managers assigned to carry out the organization's mission.

Technical excellence is also related to the strategic management of an organization's human capital. The technical excellence of its workforce is an organization's most critical asset in accomplishing its mission. Therefore, ensuring the continued development of scientific and technical expertise is necessary to preserve an organization's, and the nation's, role as a leader in technology. It is also significant to producing good standards and, accordingly, their application.

In an attempt to identify a few outstanding characteristics of managers and management approaches that would ensure a program's success, NASA, after completing the very successful Saturn-Apollo program, undertook a research study in 1974 on management philosophies as applied to major NASA programs.⁵ The study identified three "tall poles"

important to program management:

- “Pay attention to detail.” (George M. Low)
- “Leave no stone unturned.” (Wernher von Braun)
- “Be aggressive—not passive.” (Lee B. James)

These philosophies create policies and management methods that are highly conducive to program success or, in other words, technical excellence. Proven standards are a product of these efforts.

Some Examples of Technical Excellence Initiatives

In 2007, NASA undertook a technical excellence initiative to identify and resolve engineering challenges.⁶ The initiative was designed to provide quality solutions and work that will translate into an agency investment strategy for application to present and future missions. Among the attributes of this initiative are the improvement of overall technical capability; development of analysis and testing beneficial to multiple missions, programs, and projects; advancement to tool/technique capability; and proven standards.

In 2006, the aerospace industry released a position paper that argues for standards based on technical excellence of content rather than the source of a standard.⁷ Experts from the Aerospace Industries Association’s Strategic Standardization Forum for Aerospace (SSFA) prepared a position paper on the use of standards in response to growing concern that certain policies and legislation may be putting the industry—and consumers—at risk. The SSFA emphasizes that the aerospace industry must select standards based on safety, quality, and technical merit, rather than based on which organization developed them.⁸ Thus, the authors of the paper recognized technical excellence relative to ensuring that proven standards are produced and applied in order for good engineering to be achieved.

Along with cost and schedule, mass control of space systems is a primary measure of the health of a space system’s development. This can be seen by often quoted price per pound delivered to space, based on cost schedules of available launch service providers. When payloads exceed their requirements, additional costs for launch vehicle upgrades and altered launch planning can have a catastrophic effect on a payload’s programmatic success. While development of mass control standards has traditionally focused on the mass of the payload, little attention has been given to the mass and performance of the launch vehicle itself. Individually, stages of launch vehicles are subjected to traditional mass control; however the relationship between the

mass of the stage and the corresponding performance of the launch vehicle is an important contribution to technical excellence and the resulting standards. These relationships are to be addressed in upcoming revisions to both national [and] international mass control standards for space systems, and will have a meaningful effect on the development of new commercial and government launch systems.⁹

The philosophy relative to enhancing technical excellence through the interplay of standards and their use is reflected in the following by Michael Griffin, who was the NASA Administrator from 2005 to 2009:

One aspect of this discussion is the need to set certain engineering technical standards to ensure compatibility and interoperability in our exploration architecture. Analogous to my previous comments about spoken languages for future space explorers, it is important that the engineering standard for NASA's architecture be specified with the international metric, or SI, standards as the base unit of measure, with English units only by exception when it makes sense for NASA to do so. Thus, we hope for a high degree of compatibility of interfaces and standards, as space-faring nations explore the Moon, Mars, and near-Earth asteroids together.¹⁰

Thus, technical excellence is crucial to ensuring the compatibility and interoperability of a system's architecture. Proven standards, also referred to as good standards, are important to achieving this goal.

Good Standards

Perhaps it is best to again consult the dictionary for what is meant by the term "standard." It means, among other things, "a degree or level of requirement, excellence, or attainment." It is this meaning that we associate with good standards and their role in achieving the success of a program or project.

The motivations for good standards and the associated enhancement of technical excellence vary considerably. One most often sees economic issues as the principal motivation. Applications to regulatory matters are another strong motivation. Among the principal motivations for good standards are international competitiveness; commodity confidence; safeguards for health, safety, and environment; risk reduction; facilitation of commercial communications; and technology transfer. However, enhancing organizational capabilities and technical excellence, although readily recognized as a key motivation, is not often seen in the list of motivations for the development and promotion of good standards. For example, in its overview of the U.S. standardization system, the American National Standards Institute noted the following:

Within the U.S. standardization system, stakeholders—companies, government agencies, public interest organizations, and individuals—follow the method of standards

development and the conformity assessment scheme most appropriate for their particular needs. Rapidly evolving fields have requirements that are far different from those of traditional manufacturers or highly regulated technologies.¹¹

In 2012, the *World Standards Cooperation Newsletter* emphasized that

good standards are technology-independent. A good standard helps companies build products that work and communicate with each other and within existing systems safely, anywhere in the world. A good standard focuses on criteria that help industry stakeholders to consistently test and verify the safety, performance and quality of different technologies in the same space. This builds trust and is the only way how markets can grow and expand.¹²



Standardization activities establish engineering and technical applications for processes and practices and, in doing so, enhance all organizational capabilities and further promote technical excellence.

Many strong domestic and global standards developers are serving, for example, the aerospace industry. The U.S. aerospace industry has a stated policy of choosing standards based on technical merit and suitability for use rather than based on the developing organization. This practice is important to ensure the use of proven standards.

Standards are an integral part of all organizational product development efforts. Designers and development engineers should be among the most aggressive supporters of technical standards. Standardization activities establish engineering and technical applications for processes and practices and, in doing so, enhance all organizational capabilities and further promote technical excellence. Thus, they enable an organization to not dissipate its energies on the costly exercise of “reinventing the wheel.”

The integration of good standards is one step toward the goal of significantly enhancing an organization’s technical capabilities and products. Technical excellence is the key to the nation’s future in the rapidly growing globalization of industry. For the United States to remain competitive and maintain its technical leadership in the world, enhancing the nation’s capabilities is critical. These capabilities can be acquired only by achieving technical excellence, which is a requirement for good systems engineering.¹³ Good standards provide a major opportunity to achieve the goal of enhancing organizational capabilities

and providing a means whereby technical excellence can be infused into the development and manufacturing process.¹⁴

In many cases, the existing standards, or the requirements within them, are so well established that—without good examples highlighting a deficiency or weakness in the standard—it is hard to substantiate the need for a change on the basis of technical excellence.

Such was the situation facing the NASA Engineering and Safety Center's threaded fastening systems standard development team, which, over a period of about 4 years, developed and released NASA-STD-5020, "Requirements for Threaded Fastening Systems in Spaceflight Hardware." The team, comprising subject matter experts from NASA, aerospace contractors, and academia, decided in its initial meetings that it would, to the extent possible with available resources, use test data to substantiate changes to traditional requirements. One example of this was the development of a structural failure criterion for a bolt loaded in both axial tension and transverse shear (tension/shear interaction), particularly for the case of a single lap shear joint. Equations for tension/shear interaction in fasteners have been extensively published in aircraft structures manuals or text books for decades. However, the applicability of those equations to a single lap shear joint was frequently questioned, especially for the common design situation of a preloaded bolt installed into a threaded insert. Using a custom-designed fixture, a NASA program sponsored the testing of several aerospace-quality bolts at varying ratios of tension load and shear load and plotted a failure envelope to fit the data. This test program indicated that the traditional interaction equations were potentially not conservative. Therefore, the modified criterion was incorporated into a new NASA standard. Thus, as a result of technical excellence, a new and better standard was produced.

Enhancing an organization's capabilities and products is an important product of standards, especially when coupled with allied information such as lessons learned and experiences with the use of a standard. Such must be the thrust of any viable organization. This is reinforced and expanded based on feedback from an organization's staff, its contractors, and users of its products in order to improve the content of standards. Feedback, in turn, helps industry meet demands for timely, productive, and reliable systems and contributes to improvements in efficiency and costs.

Another area in which technical excellence drives the use of proven standards is model-based engineering (MBE). A National Defense Industry Association (NDIA) report¹⁵ defines MBE as an approach to engineering in which models

- are an integral part of the technical baseline;

- evolve throughout the acquisition life cycle;
- are integrated across all program disciplines (systems engineering, operations analysis, software engineering, hardware engineering, manufacturing, logistics, etc.); and
- can be shared and/or reused across acquisition programs, including between government and industry stakeholders.

The creation, management, and usage of product-related data across a cradle-to-grave life cycle are daily events at NASA. The integration and sharing of electronic product data between NASA centers, across programs and projects, and with prime contractors and subcontractors have become mission critical. The agency-wide challenge is to provide a product development capability level that is seen in many of NASA's prime contractors.

Multidisciplinary teams (such as systems engineering, product engineering, manufacturing, purchasing, operations, maintenance, and sustainment), as well as remote participants (local or globally dispersed suppliers, subcontractors, and so on), need quick access not only to the product data they are working on but also to associated information that better defines product performance, functionality, form, and fit to enable building of their products and services related to the product data.

To meet the demands of an MBE environment, the transition can be successful only if it is approached in a collaborative manner with the involvement of the government, industry, tool vendors, and academia. The NDIA report¹⁶ recognizes the need for

- developing an MBE standards road map,
- initiating a research program to close high-priority technical gaps,
- developing the standards identified in the standards road map,
- providing seed funding for the development of reference implementations of select MBE standards, and
- developing an MBE program.

Many organizations have realized that they must put proven standards in place before they can successfully evolve into an MBE environment. One such organization is PDES, Inc., which was formed in the 1980s and comprises members from industry, U.S. government agencies, universities, and software vendors. PDES supports the digital enterprise through the development and implementation of information standards to support MBE, model-based manufacturing, and model-based sustainment. Implementation testing and data exchange using the ISO 10303 standard are an integral part of PDES.

Other organizations, such as the International Council on Systems Engineering, Object Management Group, Inc., and National Institute of Standards and Technology, are collaborating in the development of rigorous, proven standards that facilitate data exchange among disparate product life-cycle management systems.

Concluding Remarks

We have endeavored to focus on the importance of standards and to provide readers with some information and motivations that will enhance their quest for technical excellence. The need for technical excellence is a significant matter for all organizations. Proven standards are an important product of technical excellence. Proven standards play an important role in the transfer of technical experiences, lessons learned, best practices, and infusion of new technology for the further enhancement of technical excellence within all organizations. Thus, not only do good standards support the achievement of technical excellence, they also enable technical excellence to be passed on to others. Although technical excellence is not easy to quantify, there is no doubt it is readily recognized, both by those involved in standards use and development activities and by those who are the “customers,” be they public, government, or industry.

¹Teresa Vanhooser, “MSFC Technical Excellence/Technical Authority,” NASA Marshall Space Flight Center, Huntsville, AL, May 2007.

²Chris Scolese, “Four Guiding Principles of Technical Excellence,” *ASK OCE*, Vol. 1, Issue 4, NASA Headquarters, Washington, DC, February 8, 2006.

³Chris Scolese, “Technical Excellence: Roles and Responsibilities,” *ASK OCE*, Vol. 1, Issue 5, NASA Headquarters, Washington, DC, February 24, 2006.

⁴“Engineering and Technology for the 21st Century: Technical Excellence,” Brigham Young University, Provo, UT, March 16, 2007.

⁵Konrad K. Dannenberg, *Management Philosophies as Applied to Major NASA Programs*, NASA-CR-141258, 1974.

⁶See Note 4.

⁷American National Standards Institute, “Aerospace Industry Argues for Standards Based on Technical Excellence Rather Than Source,” March 7, 2006.

⁸Strategic Standardization Forum for Aerospace, Aerospace Industries Association, “Safety of Aerospace Products Demands Freedom to Select Most Appropriate Standards,” <http://www.ssf-aerospace.org/>, March 2006.

⁹See Note 1.

¹⁰Michael D. Griffin, “Partnership in Space Activities” (remarks, 56th International Astronautical Congress, October 20, 2006).

¹¹American National Standards Institute, *Overview of the U.S. Standardization System: Voluntary Consensus Standards and Conformity Assessment Activities*, Third Edition, 2010.

¹²“Standards Grow Business,” *World Standards Cooperation (WSC) Newsletter*, No. 5, newsletter@worldstandardscooperation.org, August 2012.

¹³William Vaughan, “Technical Excellence: A Requirement for Good Systems Engineering,” *Defense Standardization Program Journal*, July/December 2010.

¹⁴William W. Vaughan and Paul S. Gill, “Engineering Excellence and the Role of Technical Standards” (paper AIAA-2006-0573, 44th AIAA Aerospace Sciences Meeting, 2006).

¹⁵NDIA, *Final Report of the Model Based Engineering (MBE) Subcommittee*, Final Draft, February 10, 2011.

¹⁶See Note 15.

About the Authors

William Vaughan is a research professor at the University of Alabama in Huntsville, AL, and served 10 years as director of the university’s Research Institute. Previously, he was a division chief at the NASA Marshall Space Flight Center with responsibility for the natural environment design requirements for the Saturn Apollo, Space Shuttle, and other flight programs. His standard-related experience includes participating in the development of the American Institute of Aeronautics and Astronautics Standards Program and the NASA Technical Standards Program.

Paul Gill is a technical manager in the NASA Marshall Space Flight Center’s Systems Engineering Office with responsibility for NASA’s Product Data and Life-Cycle Management Initiative. He is the former chief of the NASA Technical Standards Program. He has 15 years’ experience in the management and development of domestic and international technical standards. He also serves as the liaison for the NASA Chief Engineer on ISO Space Systems standards activities.

The authors would like to thank two people for their contributions of examples of technical excellence through the use of standards: Geoffrey Beach, NASA Aerospace Flight Systems, for his input on the mass control of space systems and Robert Wingate, NASA Structural Mechanics, for his input on NASA-STD-5020. ✨

Program News

Topical Information on Standardization Programs

DMSMS Working Group Recognizes 2013 Achievements

The Diminishing Manufacturing Sources and Material Shortages (DMSMS) achievement awards seek to recognize individuals and teams from the government who are most responsible for significant achievements in proactive DMSMS management and implementation. The awards are based on achievements in the following areas:

- Exceptional DMSMS management
- Significantly improved and quantifiable readiness levels
- Substantial cost avoidance
- Exceptional warfighter support related to or realized through mitigation of a DMSMS issue
- Creation or implementation of a DMSMS best practice that increases supportability and availability of systems to the warfighter.

This year, the DMSMS Working Group received nominations demonstrating varying levels of achievement in mitigating DMSMS. Some stood out as exemplifying extraordinary accomplishment. The evaluators (the service leads and the committee co-chairs of the DMSMS Working Group) selected three individuals and five teams as being worthy of receiving a 2013 achievement award:

■ **Individual achievement**

- * Mr. Rex Coombs, Fleet Support Team (FST), Air Combat Electronics Program Office (PMA-209), Naval Air Systems Command

Program News

- * Ms. Robin Brown, Logistics Management Analyst, DMSMS Branch, Naval Air Warfare Center Aircraft Division
- * Mr. Thomas Beckstedt, Lead Equipment Specialist, Generalized Emulation of Microcircuits (GEM) Program

■ Team achievement

- * Obsolescence Management Team, Armed Scout Helicopter (ASH) Project Management Office, Redstone Arsenal, Department of the Army
- * DMSMS Enterprise Approach, Program Executive Office Integrated Warfare Systems 2.0 (PEO IWS 2.0) and Naval Surface Warfare Center (NSWC), Crane Division
- * DMSMS Management Team, Product Manager (PdM), Radar Systems, Marine Corps Systems Command
- * Air Force DMSMS Program Office, 448 Supply Chain Management Wing, Air Force Sustainment Center
- * Advanced Medium-Range Air-to-Air Missile (AMRAAM) DMSMS Program Team, Air Dominance Division, Armament Directorate, Air Force Life Cycle Management Center, Air Force Materiel Command.

I extend my sincere congratulations and appreciation to each of you.

Gregory E. Saunders
Director
Defense Standardization Program Office

INDIVIDUAL ACHIEVEMENT AWARDS



Pictured is Mr. Rex Coombs with Mr. Stephen Welby, Deputy Assistant Secretary of Defense, Systems Engineering.

Mr. Rex Coombs guided the FST, PMA-209, Naval Air Systems Command, in the establishment of an extensive, proactive DMSMS program to manage PMA-209's broad product base with a modest staff and limited funding. His management techniques include product warehousing, hardware reuse, leveraging, reverse engineering, and parts distributor research and analysis. Mr. Coombs developed an innovative sustainability analysis process for identifying piece-part supply shortfalls and implementing mitigation actions. Use of the process has had significant positive impacts on life-cycle sustainability and prevented mission impacts, unnecessary system redesign, and costly system replacements in multiple situations. Mr. Coombs also developed a highly successful hardware reuse program that eliminates expensive product redesigns due to obsolescence, improves Navy fleet readiness, and reduces repair costs. Under Mr. Coombs's direction, the PMA-209 FST was recognized by the Defense Logistics Agency "Million Dollar Board" as the fourth biggest Navy hardware reutilization cost avoidance program (\$8.9 million cost avoidance in FY10 alone).

INDIVIDUAL ACHIEVEMENT AWARDS

Ms. Robin Brown—a logistics management analyst in the DMSMS Branch, Naval Air Warfare Center Aircraft Division—has assisted all Naval Air Systems Command (NAVAIR) program offices with establishing DMSMS management programs. She has been instrumental in the completion and approval of many program office DMSMS plans, ensuring they are true representations of DMSMS processes and procedures, while incorporating the fundamental tenets of DMSMS/obsolescence management. Further, she has helped many program offices achieve their goals in a much shorter time frame, saving time and money. Ms. Brown also has been supporting the NAVAIR DMSMS Branch since 2004 and was instrumental in creating the NAVAIR DMSMS Working Group (NDWG). She facilitates NDWG meetings, bringing together DMSMS representatives from NAVAIR programs to foster collaboration, share lessons learned and best practices, address policy, provide training opportunities, identify and address recurring DMSMS-related challenges, and define or revise processes to manage and mitigate the impact of DMSMS. Ms. Brown’s contributions have helped increase supportability and availability of systems to the warfighter.



Pictured is Ms. Robin Brown with Mr. Stephen Welby.

Mr. Thomas Beckstedt—the principal assistant to the GEM program manager and the lead equipment specialist—applies his expertise in all aspects of microcircuit fabrication and associated logistics to ensure that money is not wasted pursuing microcircuit emulations when other valid sources or alternative means of support are available. When microcircuit emulation is necessary, Mr. Beckstedt follows the project from its start until the microcircuit is successfully manufactured, tested as a component, integrated in the system, and delivered to the requiring activity. He ensures that problems are successfully solved and that the total item record in the Federal Logistics Information System is updated. Depending on the device type, he may update a standard microcircuit drawing, the Standard Microcircuit Cross-Reference, and the qualified manufacturers list. Mr. Beckstedt’s job is complex, and only someone with his years of experience and expertise could successfully integrate with industry and government engineers and logisticians to solve complex microcircuit issues through the GEM program.



Pictured is Mr. Thomas Beckstedt.

TEAM ACHIEVEMENT AWARDS

The **Obsolescence Management Team for the ASH Project Management Office, Redstone Arsenal**, Department of the Army, established a proactive obsolescence program covering both the OH-58D Kiowa Warrior helicopter and its replacement, the OH-58F. Overcoming the challenges of supporting two configurations of an aircraft in different phases of the life cycle required collaboration with multiple suppliers to support multiple line replaceable units (LRUs) for new production, sustainment, and so on; with the Kiowa Warrior Product Office; and with the LRUs' multiple managing entities, including several Army commands, the Navy, and the Defense Logistics Agency. The team—through its obsolescence working groups (OWGs)—has resolved numerous DMS/obsolescence issues, ensuring that the original equipment manufacturers (OEMs) have enough spare parts. The OWGs, with OEM participation, seek to identify DMS/obsolescence risk early by, for example, continually monitoring component life projects based on supplier-provided data. Early identification of risk allows for more time to develop cost-effective solutions and to execute mitigation actions before the program is negatively affected.



© Denise DeMonia, Armed Scout Helicopter Project Office

Pictured are, left to right, Mr. Brett Addington, Mr. George Lewis, Mr. Kelly Ward, Mr. Scott Dunlap, and Mr. Thomas Fitzgerald.

A **PEO IWS 2.0 and NSWC, Crane Division, team** collaborated to develop a consistent, cost-effective enterprise approach to DMSMS management for all PEO IWS 2.0 sensor systems. The team evaluated system needs across the enterprise to ensure the appropriate allocation of resources and an optimal level of DMSMS support. Through substantial collaboration with project managers, in-service engineering agents, and DMSMS experts, the team implemented best practices, standardized processes and methods, and established clear roles and responsibilities for DMSMS working groups. Furthermore, the team dedicated a substantial portion of the effort toward developing a simplified analysis and report format to meaningfully represent the DMSMS health of the systems to the program office, enabling it to prioritize and make decisions about DMSMS mitigations at a high level. NSWC Crane is managing the DMSMS infrastructure required to monitor and mitigate obsolescence for approximately 10,000 components and commercial off-the-shelf items affecting PEO IWS 2.0 systems.



Pictured are, left to right, Ms. Alyssa Robertson, Ms. Kelly Kitcoff, Mr. Daniel Horstman, Ms. Misty Neukam, and Mr. Keith Meyer. Missing from the picture are Mr. Larry Barry, Ms. Amanda Perry, Ms. Kendra Norris, Mr. Nick Gates, Mr. Stephan Graves, Mr. Isaiah Mullis, Mr. Mike Baum, Ms. Nova Carden, and Mr. Chris Sims.

TEAM ACHIEVEMENT AWARDS

The **DMSMS Management Team, PdM, Radar Systems**, Marine Corps Systems Command, addressed numerous DMSMS and life-cycle issues with obsolete major components of radar systems used to acquire and sustain command, control, and communications and to counter mortar, artillery, and rocket fire. The team managed a diverse portfolio, valued at more than \$133 million, and implemented technology refreshes and engineering changes to sustain the AN/TPS-59A(V)3, the AN/TPS-63B, and the Family of Target Acquisition Systems (FTAS) to end of life. The AN/TPS-59 team implemented eight separate technical refreshes addressing the DMSMS obsolescence of critical major components, with planned fielding in FY14–16. The AN/TPS-63 team successfully fielded an RF Suite Receiver assembly that returned the radar's performance range from the degraded 80 miles to the performance specification of 160 miles. The FTAS team completed the refresh and fielding of 29 AN/TPQ-49 systems. These combined efforts resolved immediate and emerging DMSMS issues, increased reliability and readiness, and ensured the continued availability of these critical assets.



Pictured are, left to right, Mr. John Mindzak, Captain Frank Mello, CWO-3 Dwayne Fort, and Mr. William Davidson. Missing from the picture are Mr. Jason Choi, Mr. Willie Currie, Gunnery Sergeant Jeffery Cox, Mr. Tom Drent, Mr. Richard Frank, Mr. Edward Garrison, Mr. John Garvey, Ms. Cathy Henderson, Mr. Hondo Shaver, Mr. Jim Kehn, Mr. Phillip Kenoyer, Mr. Kevin Luc, Mr. John Magerowski, Mr. Telyvin Murphy, Ms. Katherine Miller, Mr. Scott Neal, Mr. Joey Rancourt, Mr. Todd Shull, Mr. Damon Trevithick, Mr. Lorin Watts, and Mr. Kenneth VanZandt.

The **Air Force DMSMS Program Office**, 448 Supply Chain Management Wing, Air Force Sustainment Center, established a single enterprise-wide DMSMS program that has demonstrated an exceptional standard of obsolescence prevention and resolution while improving the program's cost-effectiveness and efficiency. One of the DMSMS team's actions was to consolidate all Air Force requirements into a single DMSMS predictive tool database, eliminating the costs of administering multiple DMSMS tool contracts, eliminating duplication of effort, enabling sharing of information across all platforms, and avoiding costs of more than \$150 million. The team also awarded a consolidated Air Force-wide analysis and resolution contract, which provided \$3.3 million in cost savings and improved efficiency by standardizing DMSMS processes across the enterprise. In addition, the team streamlined the shared data warehouse process by reducing multiple focal points to one centralized focal point. The new process resulted in the completion of 178 worksheets, allowing the Defense Logistics Agency sufficient time to purchase life-of-type buys to support 276 next higher assemblies.



Pictured are, left to right, Mr. Royce Smith, Ms. Debra Shepherd-Moore, Mr. Jeremy Scoles, Mr. Sim Tran, and Mr. Brent Skeen.

TEAM ACHIEVEMENT AWARDS

The **AMRAAM DMSMS Program Team**—within the Air Dominance Division, Armament Directorate, Air Force Life Cycle Management Center, Air Force Materiel Command—adopted a number of aggressive, proactive strategies to mitigate DMSMS issues and avoid serious risks to production of the AMRAAM. Among them are a program to manage life-of-type buys to link the exhaustion of a legacy part with the introduction of a new part; a circuit/circuit card assembly replacement program to redesign assemblies when a replacement part is physically larger, requires more power, or generates more heat than the obsolescent part; and a processor replacement program to design, integrate, and produce a common board replacement assembly. The team's proactive approach has resulted in significant cost avoidance and a healthy and sustainable production capability. Further, the team and the prime contractor have forged a highly cohesive team to ensure issues continue to be proactively managed to maintain the lowest total cost of ownership throughout the product life cycle.



Pictured are, left to right, Ms. Gail Mitchell, Mr. Bob McFarland, Ms. Melissa St. Vincent, Mr. Al Iannaccone, Mr. Robert Simmons, Mr. Lynn Stockbridge, Mr. Dennis Irons, Mr. Ben Collins, Mr. Mark Kunz, Mr. Kim Crockett, Mr. Eric Duron, Ms. Irene Easterday, and Mr. Steve Thompson. Missing from the picture are Mr. Nathan Pappas, Mr. Dan White, Mr. Bill Rones, Mr. Brian Stewart, Mr. Jeff Mixson, Mr. Philip Herzog, Mr. Bill Whittenburg, and Ms. Valerie Skinner.



Events

Upcoming Events and Information

June 30–July 3, 2014, Las Vegas, NV
24th Annual INCOSE International Symposium

The International Council on Systems Engineering's (INCOSE's) International Symposium is the premier international forum for systems engineering. Participants network; share ideas, knowledge, and practices; and learn about the most recent innovations, trends, experiences, and issues in systems engineering. Presentations and tutorials will address ways in which systems engineering principles, processes, and perspectives are performed today and how systems engineering may influence our future. Topics include technology insertion, process improvements, and organizational governance of the systems we make, manage, operate, and maintain over their life cycle. INCOSE's 2014 International Symposium will be held at the Greenvalley Ranch Resort, Las Vegas, NV. For more information on this event, go to <http://www.incose.org/symp2014/>.

August 11–14, 2014, Ottawa, ON, Canada
63rd Annual SES Conference

The Standards Engineering Society (SES) will host its 63rd Annual Conference at the

Fairmont Chateau Laurier, in Ottawa, Ontario. The theme of this conference is "Standardization and Conformity Assessment Across Borders." SES is pleased to announce that John Walter, chief executive officer of the Standards Council of Canada, will be the keynote speaker at the conference. For more information, go to www.ses-standards.org and click "Annual Conference."

September 8–12, 2014, Orlando, FL
2014 SISO Fall Simulation Interoperability Workshop

The Simulation Interoperability Standards Organization (SISO) will hold its fall 2014 Simulation Interoperability Workshop at the Florida Mall Conference Center in Orlando, FL. The workshop is a semiannual event encompassing a broad range of model and simulation issues, applications, and communities. The workshop consists of a series of forums and special sessions addressing interoperability issues and proposed solutions; tutorials on state-of-the-art methods, tools, and techniques; and exhibits displaying the latest technological advances. For more information, go to www.sisostds.org and click "Upcoming News/Events."



Events

Upcoming Events and Information

October 23, 2014, Washington, DC

U.S. Celebration of World Standards Day 2014

The U.S. Celebration of World Standards Day will be held at the Fairmont Hotel in Washington, DC. This year's theme—Standards Level the Playing Field—focuses on how standards stimulate trade and overcome artificial trade barriers, helping to make companies, industries, and economies more competitive. The event is sponsored by the American National Standards Institute (ANSI). For more information on the event or to register, go to https://eseries.ansi.org/source/Events/Event.cfm?EVENT=WSD_14, or go to www.ansi.org, click “Meetings & Events,” and then click “Upcoming ANSI Events.”

October 27–30, 2014, Springfield, VA

17th Annual NDIA Systems Engineering Conference

This year's Systems Engineering Conference will be held at the Waterford Conference Center in Springfield, VA. The focus of the conference is on improving acquisition and performance of defense programs and systems, including network-centric

operations and data/information interoperability, systems engineering, and all aspects of system sustainment. The conference is sponsored by the Systems Engineering Division of National Defense Industrial Association (NDIA) and is supported by the Deputy Assistant Secretary of Defense for Systems Engineering, the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, and the Office of the DoD Chief Information Officer. For more information, please go to www.ndia.org and click “Meetings and Events.”

December 1–4, 2014, San Antonio, TX

2014 DMSMS Conference

The 2014 Diminishing Manufacturing Sources and Material Shortages (DMSMS) Conference will be held at the Grand Hyatt San Antonio and the Henry B. Gonzalez Convention Center in San Antonio, TX. Details on the technical program are still being worked out, but the event promises to be top-notch in every way. For more information on the event, go to www.dmsmsmeetings.com.



People

People in the Standardization Community

Welcome

Gordon Gillerman assumed the position of acting director of the Standards Coordination Office at the National Institute of Standards and Technology (NIST). Previously, Mr. Gillerman was the chief of the Standards Services Division/Technology Services at NIST. The Standards Services Division advises federal agencies and works with U.S. industry and other stakeholders on domestic and global standards and conformity assessment policy.

Farewell

George Arnold retired from NIST at the end of May to pursue a unique opportunity in the private sector. While at NIST, Mr. Arnold served in various roles, including as the national coordinator for smart grid interoperability and as the director of the Standards Coordination Office. We wish him well in his new position.

Defense Parts Management Portal–DPMP

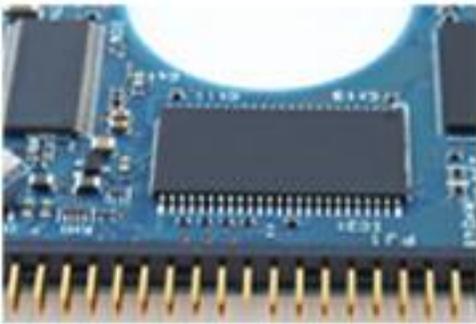
The DPMP is a new public website brought to you by the Parts Standardization and Management Committee (PSMC) to serve the defense parts management community.

The DPMP is a new resource, a new marketplace, and a “one-stop shop” for parts management resources. It is a navigation tool, a communication and collaboration resource, and an information exchange. It gives you quick and easy access to the resources you need, saves you time and money, connects you to new customers or suppliers, and assists you with finding the answers you need.

This dynamic website will grow and be shaped by its member organizations. A new and innovative feature of the DPMP is its use of “bridge pages.” Organizations with interests in parts and components are invited to become DPMP members by taking control of a bridge page. Chances are good that your organization is already listed in the DPMP.

There is no cost.

Explore the DPMP at <https://dpmp.lmi.org>. For more information, look at the documents under “Learn more about the DPMP.” Click “Contact Us” to send us your questions or comments.



Upcoming Issues Call for Contributors

We are always seeking articles that relate to our themes or other standardization topics. We invite anyone involved in standardization—government employees, military personnel, industry leaders, members of academia, and others—to submit proposed articles for use in the *DSP Journal*. Please let us know if you would like to contribute.

Following are our themes for upcoming issues:

Issue	Theme
January/March 2014	Qualification/Conformity Assessment
April/June 2014	Standardization Stars

If you have ideas for articles or want more information, contact Tim Koczanski, Editor, *DSP Journal*, Defense Standardization Program Office, 8725 John J. Kingman Road, STOP 5100, Fort Belvoir, VA 22060-6220 or e-mail DSP-Editor@dla.mil.

Our office reserves the right to modify or reject any submission as deemed appropriate. We will be glad to send out our editorial guidelines and work with any author to get his or her material shaped into an article.



