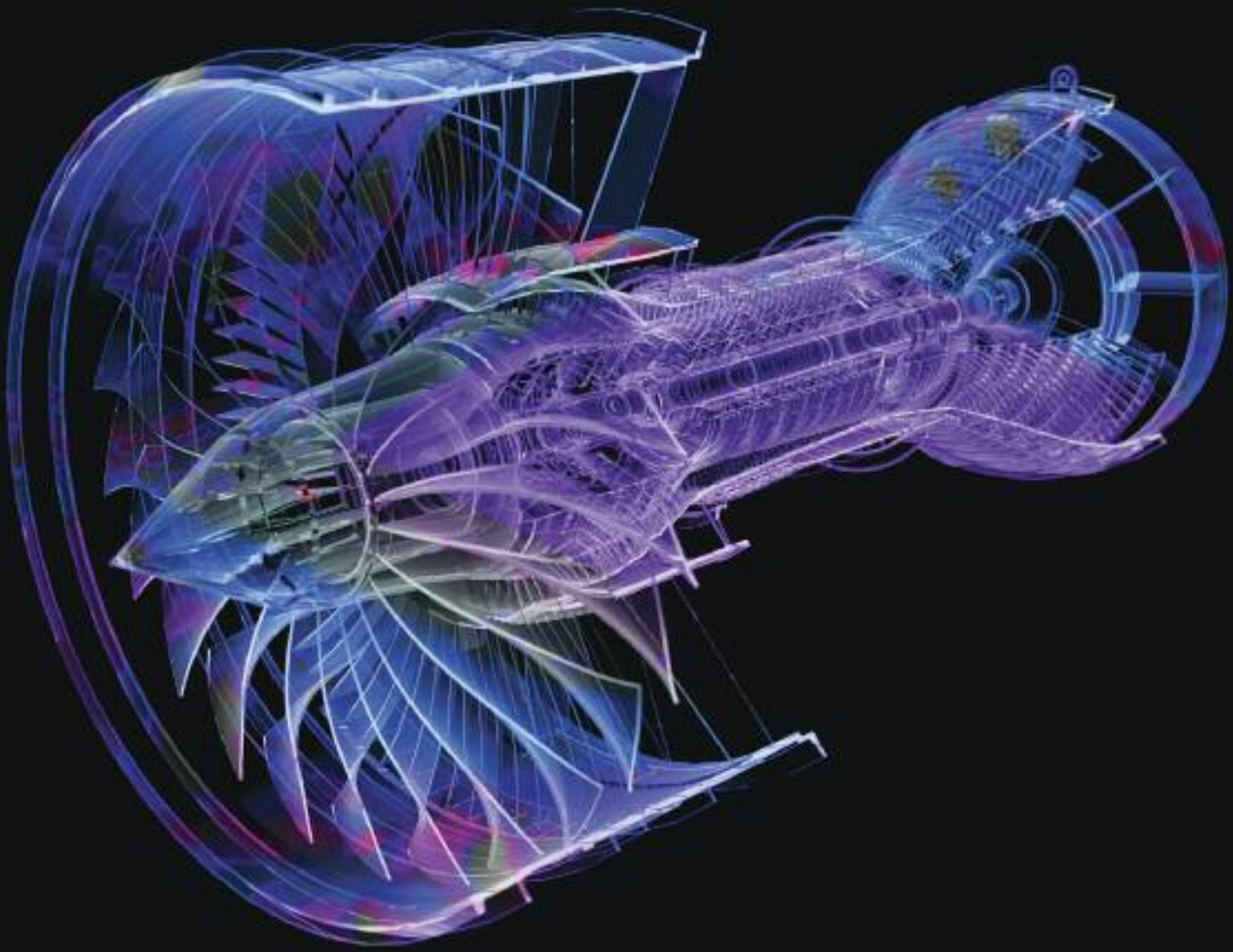
GIDEP Helps Mitigate the Risk of Counterfeits

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.

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.

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

[2]Carl 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.

[3]Department 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.