



Defense Standardization Program

Journal

January/March 2014

Qualification and Conformity Assessment

The DoD Qualification Program
Configuration Management Best Practices
DoD: Collaborating with Industry to Improve Quality
Better Training for Better Defense
Anticounterfeit Best Practices



1 Director's Forum

3 The DoD Qualification Program

9 Configuration Management Best Practices

17 DoD: Collaborating with Industry to Improve Quality

23 Better Training for Better Defense

Using Personnel Credentialing Standards and Conformity Assessment to Improve National Security

29 Anticounterfeit Best Practices



Departments

38 Program News

41 Events

43 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@dla.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



At Ford, “Quality is Job 1.”

Anybody who knows me knows I’m a car guy. You can see it in my office where there are racing pictures, a stand showing all seven traditional racing flags (from green to checker), and a number of car models, including die-casts of my beloved Nissan 300ZX twin turbo and my recent Corvette Z06. (My new Stingray model hasn’t arrived yet).

Car guys pay attention to car ads. One of the ads that sticks out in my mind was from the 1980s, when Ford found itself going head to head with Japanese imports. At that time, auto manufacturers like Toyota began flooding the U.S. market with well-built, high-quality cars, and domestic automakers were losing market share. There was a perception that U.S. manufacturers were producing cars that were of lower quality than those coming from Japan. In order to compete, Ford launched the advertising campaign, “At Ford, Quality is Job 1.” Clearly, they were looking to reassure the U.S. car-buying public that domestic manufacturers could still turn out a quality vehicle and remain competitive, even in the face of highly publicized issues such as an exploding gas tank, the park-to-reverse transmission defect, and alleged roll-over instability on certain models. The slogan, “Quality is Job 1,” was meant to demonstrate that Ford got it and to showcase the Ford of the future, not the Ford of the past.

Ford chose its slogan well. “Quality” is defined as high grade, superiority, or excellence. This was the one word that the advertising executives could use to cover all that upper management wanted Ford to be. Quality referred not only to labor and materials, but also to the engineering and manufacturing processes that would be responsible for turning out a better vehicle.

But what did Ford mean when it talked about quality? What comes to the mind of the buying public? What makes one car “quality” and another not so much?

Some aspects of quality seem to be subjective; some things have a look or feel or even sound of quality that is very hard to describe



Gregory E. Saunders
Director
Defense Standardization Program Office

and even harder to measure. But they don't just happen. You wouldn't believe how much engineering goes into making the satisfying "thunk" sound of a solid car door closing. There is little in modern manufacturing that is not carefully engineered. And quality is designed and manufactured into the product, and checked down to the gnat's eyebrow.

Assessing quality is one of the cornerstones of manufacturing, and it plays an important role in the development of any product. Ensuring an item will meet or exceed the requirements set forth in the specification will determine how successful overall outcomes will be. Among a number of ways that DoD tries to ensure quality are programs such as product qualification, manufacturer qualification, and other conformity assessment activities. These programs offer structure and discipline both for assessing manufacturer capability and for maintaining accurate records for use in making buying decisions.

The DoD qualification program was established to ensure the availability of frequently used items requiring long testing periods and of expensive or hard-to-come-by testing equipment. The purpose of qualification is to ensure product performance, quality, and reliability by conducting long or highly complex evaluations and tests prior to, and independent of, procurement. Our highly automated qualified products database—an amalgamation of the old qualified products lists (QPLs) and qualified manufacturers lists—helps to ensure continued availability of products in spite of the long tests required. DoD prepares, coordinates, and maintains more than 750 military specifications that call for such qualification for items that have unique military characteristics.

In addition, DoD specification preparing activities have partnered with industry to develop programs such as the Performance Review Institute's industry-managed QPL program. The idea is to invoke procedures in a commercially run program, similar to those of our qualification program, to ensure necessary quality in commercial or dual-use products. The industry-managed program is a collaborative effort involving a mix of stakeholders: suppliers, industry, and government entities. Not only do those stakeholders have an interest in product quality, but they also want to be able to leverage the industry-managed platform as a way to reduce qualification infrastructure costs and to share the burden across the industry.

Was Ford successful at making quality "Job 1"? Was it successful in convincing people that it now focused on producing a quality car—from design to engineering to manufacture to assembly—and even to support? All I can offer is that Ford has become one of the darlings in the automotive press in terms of turning out high-quality vehicles—and it's not just advertising hype. (Full disclosure: I'm a bowtie guy having just purchased a new Corvette Stingray.) Perhaps it was making quality a priority on all levels that led to the turnaround. Will there be troubles in the future? Almost without question. They will occur at virtually any large manufacturing enterprise. And no doubt, DoD will also be accused of not paying sufficient attention to quality at some point. What we must do is continue our vigilant assessment of quality.

Quality is always a work in progress.

The DoD Qualification Program

By Tim Koczanski



The Cataloging and Standardization Act of 1952 was established to provide for an economical, efficient, and effective supply management organization within DoD through the establishment of a single supply cataloging system, the standardization of supplies, and the more efficient use of supply testing, inspection, packaging, and acceptance facilities and services. DSP continues to carry out that mission enacted so many years ago. Today, one of the cornerstones of DSP is the DoD qualification program. The qualification program helps DoD meet its needs by improving the availability of products, and it assists with shortening the procurement process by completing long, or highly complex, evaluations and tests of manufacturers or products before a contract is awarded. By eliminating repetitive surveillance audits and tests, the DoD qualification program has been successful at helping to reduce costs.

What Is Qualification?

Qualification is a process performed in advance of, and independent of, an acquisition. Its purpose is either to establish, by testing, that specific products conform to the requirements in military specifications or to certify, usually by audit, a manufacturer's capability to produce qualified products. Products approved by testing are listed on a qualified products list (QPL). Products approved by the audit process are listed on a qualified manufacturers list (QML). Increasingly, these records are stored electronically in the qualified products database (QPD). The QPD can be accessed by logging onto the ASSIST database at <https://assist.dla.mil/>.

Qualified Products Lists vs. Qualified Manufacturers Lists

A QPL contains qualifying products or families of products and the sources from which the products can be procured. A QPL is normally used for items with a stable design or composition that will be continually available for an extended period of time, thereby making it practical to qualify individual products without incurring prohibitive testing costs. A product that meets the established qualification requirements is listed on an electronic QPL.

In contrast, a QML focuses on qualifying an envelope of a manufacturer's processes and materials rather than individual products. A QML is especially useful for items that experience very rapid technological advances or that have myriad variations or custom designs that would make individual product qualification impractical or excessively expensive. A QML applies to products that

- do not have recognized industry part numbers;
- are procured to a specification that covers a wide range of technologies, such as hybrid microcircuits; and

■ are part of a family of products with similar characteristics, such as printed wiring boards.

With QMLs, representative worst-case test vehicles or representative samples that contain all potential combinations of materials and processes used during production are carefully examined to determine acceptability limits. As evidence that a manufacturer's envelope of processes and materials meets the established qualification requirements, all the acceptable processes and materials are listed on the electronic QML in the QPD.

The intent of the DoD qualification program is to allow manufacturers to provide, and purchasers to obtain, satisfactory precontractual evidence that a product, or a family of products, has been tested and has met the requirements of the governing specification. By prequalifying products and sources, qualification reduces acquisition lead-times. Qualification also reduces the cost of testing by eliminating the need for redundant first-article testing, which is especially important when tests are very expensive or take a long time to conduct.

In summary, qualification optimizes the relationship between engineering risk and quality assurance costs, improves readiness through continuous availability of reliable products from viable suppliers, establishes and standardizes the requirements for evidence of manufacturers' capabilities in advance of acquisition, and establishes long-term relationships with suppliers to ensure continuous conformance to requirements and continuous product quality improvements.

What the DoD qualification program does not do is relieve suppliers of their contractual obligations to deliver items meeting all specification requirements. The program does not guarantee acceptability under a contract, nor does it waive any requirements for inspections or for maintaining quality control measures satisfactory to the government. In addition, the DoD qualification program does not relieve the original equipment manufacturer of the contractual obligation to ensure that delivered items (including the qualified items used in the equipment) comply with all specification requirements.

Paperless Initiative

Formerly, QPLs and QMLs were published as printed documents. Whenever a list changed, a revised publication (QPL or QML) was issued to update the products or sources. In addition to the technical requirements for qualification outlined in each governing specification, each qualifying activity develops its own administrative procedures to manage the initial qualification of products and sources, as well as the retention of previously qualified products and sources on a QPL or QML.

Because of limitations in engineering support, some qualifying activities may consider adding new products or sources only during a regularly scheduled review. For most QPLs, this review occurs every 24 months, as established by policy in DoD 4120.24-M, “DoD Standardization Program (DSP) Procedures.” DoD policy requires that the qualifying activities manage QPLs to ensure that previously qualified sources are still viable. Sometimes all that is required is for a management official at a manufacturing plant to certify that the products on the list are still produced and that the manufacturer has not altered the manufacturing processes or materials. If the manufacturer has made some changes, then the qualifying activity may request that the manufacturer submit new test data in order to be retained on the QPL. For certain more dynamic technologies, such as those covered by QMLs, the qualifying activity may make changes weekly. Yet, because of the administrative lead-time to publish a new paper QML, those changes were not accessible to the general user population for months.

Now, with the development of the QPD—a fully automated system—users have immediate access to all qualification data, including new and newly updated QPLs and QMLs, and DoD qualifying activities have the flexibility to publish changes as needed and to deliver those changes in near real time. Moreover, the QPD has transformed the processes for building and maintaining QPLs and QMLs by providing the qualifying activities with tools to relieve them of some of the important administrative tasks associated with managing QPLs. Among other things, the QPD does the following:

- Generates automatic alert notifications to the qualifying activity administrator when it is time for previously approved sources to certify for retention on a QPL.
- Provides validation checks to ensure that a QPL is properly prepared before it is published.
- Automatically tracks manufacturers’ addresses by pulling address information from the System for Award Management (SAM) database, and alerts the qualifying activity if a listed manufacturer’s address changes. This is important, because a manufacturer’s move to a new production facility could prompt the qualifying activity to reevaluate the manufacturer, which may involve requiring the manufacturer to provide new test data or to submit to an audit to be retained on a QPL or QML.
- Alerts qualifying activities if a Commercial and Government Entity (CAGE) code is no longer in an “Active” status in the SAM database. This could prompt the activity to investigate to ensure that the supplier has not been suspended or debarred.

The QPD has also significantly improved the management of DoD QPLs. Some reports were designed to provide some oversight and insight for management officials in the military departments, the Defense Logistics Agency, and DSPO. For example, it is

now very easy to generate a list of all QPLs with no approved sources or with only one approved source. This is important information for management, because one of the goals of the DoD qualification program is to promote competition, not to limit it. If a specification has had a qualification requirement for many years and there are still no approved sources, then perhaps the specification needs to be reviewed and modified, either to remove the qualification requirement and replace it with a requirement for first-article testing or perhaps to change the specification so that producers can meet the requirements.

In addition, several reports have been designed specifically to help suppliers meet their periodic certification requirements for retention on a QPL. For example, one report—“Manufacturers Parts by CAGE Code”—allows a manufacturer to enter its CAGE code and produce a list of all parts associated with that CAGE code on a QPL. The report also provides a drop-down list that identifies all of the QPLs containing a particular CAGE code. The report may then be exported, either in PDF or as a Microsoft Excel spreadsheet. This is a particularly useful report when a manufacturer has an extremely large number of parts on a QPL. A manufacturer can annotate changes on this file and submit it to the qualifying activity along with its periodic certification. By automating certain tasks and by designing special reports, the QPD can help qualifying activities keep their assigned QPLs up to date.



Qualification data can be accessed through the ASSIST, Quick Search, and assistdocs.com databases, which allow users to pull up data related to a QPL or QML directly from the QPD.

Accessing Qualification Data

Qualification data can be accessed through the ASSIST, Quick Search, and assistdocs.com databases, which allow users to pull up data related to a QPL or QML directly from the QPD. The data can be accessed from the Document Details page of either the QPL or QML, or from the associated governing specification, in any of those three databases.

Users who log on to ASSIST (<https://assist.dla.mil>) to access the QPD may use a variety of search options, such as searching by the government’s or manufacturer’s designa-

tion, specification number, Federal Supply Class, title, or name of the supplier. Users may also access some very useful reports. Besides “Manufacturers Designation by CAGE Code,” users looking for a national stock number (NSN) can view “Government Designation by NSN” to see if an NSN is associated with a qualified part. Many parts on a QPL are not assigned NSNs, because they may not be directly purchased by federal activities. However, if the NSN is associated with a government part on a QPL, then the user may select “Manufacturers by Government Designation” to generate a list of all qualified sources for a specific government part. Other reports provided by the QPD include “Published QPL,” “QPL to Manufacturer,” and “Suppliers by QPL Number,” just to name a few.

This fully automated system has revolutionized the DoD qualification program. To ensure that the QPD continues to meet the needs of the people who manage the qualification process and the users who rely on the information, we continually look to make improvements based on feedback from both the qualifying activities and users.

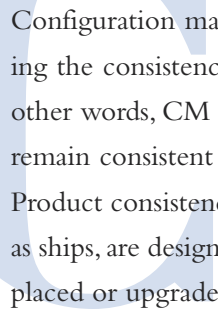
For more information about the DoD qualification program, please contact Tim Koczanski at 703-767-6870 or Tim.Koczanski@dla.mil.

About the Author

Tim Koczanski is a member of the DSPO staff. He is a program analyst and is the program manager for the DoD qualification program. ✨

Configuration Management Best Practices

By Denise Duncan and Al Lager



Configuration management (CM) is a systematic process for establishing and maintaining the consistency of a product—such as a part or component—throughout its life. In other words, CM ensures that a product’s functional performance and physical attributes remain consistent with its design and operational requirements throughout its life cycle. Product consistency is particularly important for DoD, because many of its systems, such as ships, are designed to be used for decades. Parts and components, however, must be replaced or upgraded periodically.

Possibly the first user of CM in the production of U.S. military equipment was Eli Whitney (the inventor of the cotton gin). In 1798, he started a business to manufacture muskets for the Army. He used an innovative technique to revolutionize the manufacturing process. Specifically, he fabricated interchangeable parts rather than fabricating one complete musket at a time. This approach would not have worked without employing this rudimentary form of configuration control, a major function of what we now know as configuration management.

Over time, CM practices have evolved, and DoD’s guidance has evolved along with them. The current version of DoD 5000.02¹ requires program managers (PMs) to

use a configuration management approach to establish and control product attributes and the technical baseline across the total system life cycle. This approach will identify, document, audit, and control the functional and physical characteristics of the system design; track any changes; provide an audit trail of program design decisions and design modifications; be integrated with the Systems Engineering Plan and technical planning; and be consistent with the Intellectual Property Strategy.

A wide variety of guidance is available to help PMs implement a successful CM program. That guidance is contained in standards, handbooks, and tools, such as the following:

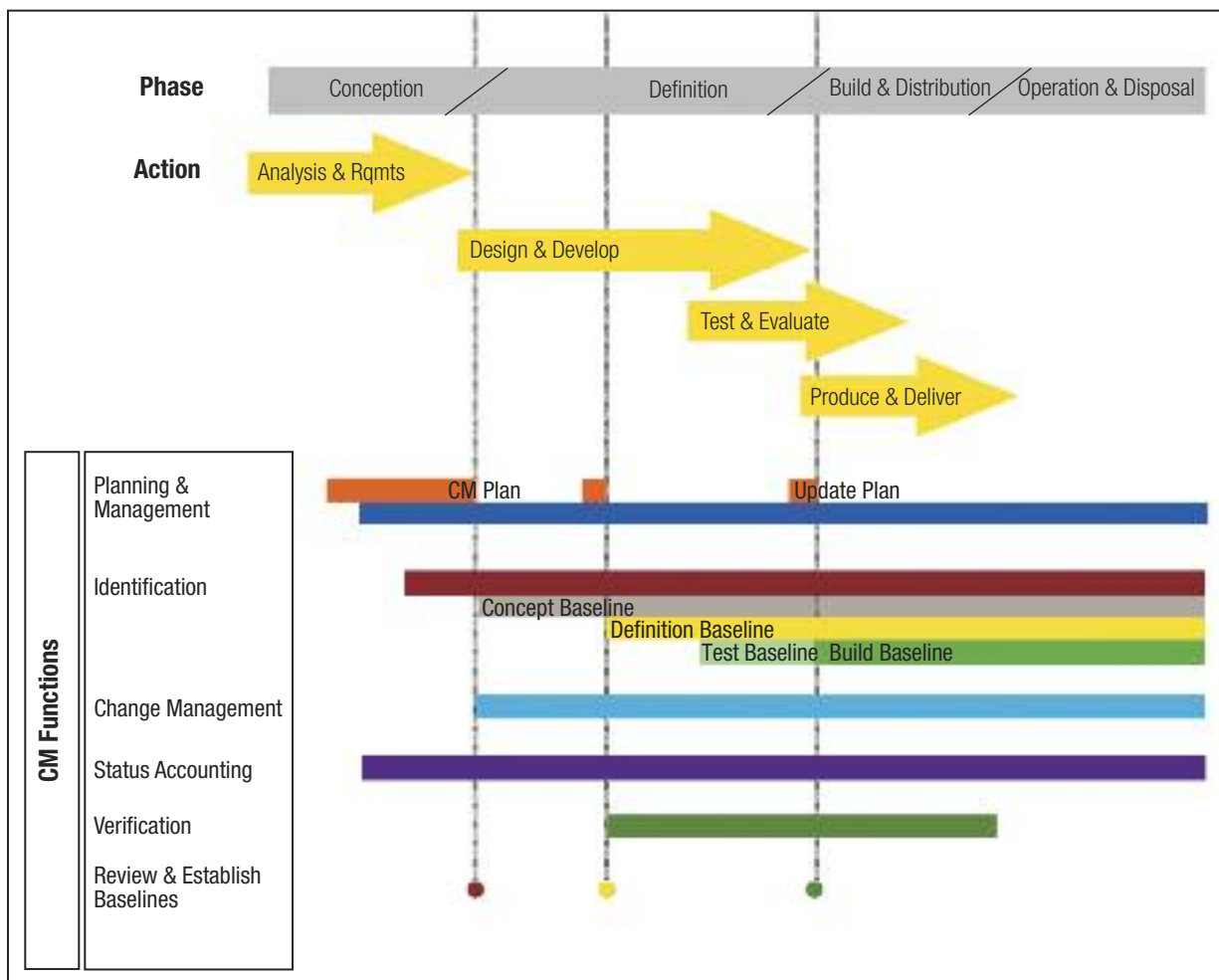
- EIA-649-B, “National Consensus Standard for Configuration Management”
- GEIA-HB-649A, *Implementation Guide for Configuration Management*
- EIA-649-1, “Configuration Management Requirements for Defense Contracts”
- MIL-HDBK-61A, *Configuration Management Guidance*
- EIA-836, “Configuration Management—Data Exchange and Interoperability”
- MIL-STD-961, “Defense and Program-Unique Specifications Format and Content”
- MIL-STD-31000A, “Technical Data Packages”
- *Configuration Management Advisor*, an online resource maintained by the Naval Air Warfare Center, Training Systems Division
- *Acquisition Community Connection*, an online resource, including a Configuration Management Plan Template, maintained by the Defense Acquisition University.

This article summarizes best practices from successful, experienced configuration managers, organized by five functions inherent in CM:

- CM planning and management
- Configuration identification
- Configuration change management
- Configuration status accounting
- Configuration verification and audit.

All five CM functions are necessary to some degree for all products. A robust CM approach is required for a complex product, such as an electronic system, a military weapon, or other product that must be supported over the product's complete life cycle. Figure 1 shows how CM works across the product life cycle. Simpler CM techniques may be used for a noncomplex product as long as they maintain the needed consistency between essential requirements, product configuration information, and the product.

Figure 1. CM across the Product Life Cycle



CM Planning and Management

From the early phases of the product life cycle, the PM and the configuration manager must determine the appropriate application of CM functions throughout the product life cycle. By identifying the context and environment of the product, they can appropriately tailor the application of CM based on things like the product requirements, complexity, and life-cycle environment.

A best practice for this CM function is to prepare a CM plan that reflects the efficient application of CM principles and practices over the product's life cycle. The CM plan should cover the following topics:

- General product definition and scope
- Description of CM activities and procedures for each major CM function
- Organization, roles, responsibilities, and resources
- Definitions of terms
- Programmatic and organizational interfaces
- Deliverables, milestones, and schedules
- Subcontract flow-down requirements.

Configuration Identification

Configuration identification is the process of identifying and documenting the attributes (functional and physical characteristics) of items that are to be placed under configuration control. Configuration identification includes the selection (identification) of configuration items (CIs), including computer software configuration items (CSCIs); determining the types of configuration documentation required for each CI/CSCI; assigning unique identifiers to each CI/CSCI and the technical documentation describing its configuration; and the establishment of configuration baselines. A hierarchical structure should be established that identifies and summarizes the CIs/CSCIs constituting a given project, product, or automated system.

To perform this function, the configuration manager must establish the product structure, determine and document the configuration items, and define the item identification scheme, that is, what characters or markings will be used and how they will be assigned to configuration items, their subordinate parts, and their associated documents.

One of the best practices in this CM function is to ensure that the identification scheme covers both developmental and final versions of configuration items, including hardware, software, documents, and procedures. The scheme must relate items at lower levels in the hierarchy to the items at which requests for change will be addressed (i.e., configuration items), and it must address the effect on associated CIs, support, training,

and maintenance equipment, as well as on associated electronic media, computer files, documents, and software components. In addition, the scheme should include version, revision, and other important status information about each item.

An important best practice in software CM is to ensure that products delivered to the customer are all placed under CM. This includes software requirements, software design, code, build scripts, software test procedures and documents, and any items that are identified with or required to create, test, operate, and maintain the software products, such as the compiler, vendor-supplied/government-furnished information, and so on.

Configuration Change Management

Change management (also called configuration control) consists of the evaluation, coordination, approval or disapproval, and implementation of changes to CIs/CSCIs after they are formally baselined. Effective change management depends on placing products under control by employing mechanisms that ensure proposed changes are properly identified, prioritized, documented, coordinated, evaluated, and adjudicated.

Once a change is approved, it must be fully documented, implemented, verified, and monitored to ensure its incorporation in all applicable systems and products. Changes identified during ongoing maintenance of products or systems in operation or production cycle forward into new requirements for appropriate analysis and entry into the change management process. In other words, they become new requests for change.

A change (or configuration) control board (CCB) is the preferred forum both for establishing CM baselines and for approving/disapproving subsequent changes to those baselines. A CCB may exist at the enterprise (customer and contractor) level, project level, or both, as defined in its charter and operating procedures.

One of the best practices in this CM function is to design the change evaluation and coordination process to be repeatable and to cover a wide variety of proposed changes. For example, the process should consider things such as the following:

- Cost or savings to both the supplier and customer
- Current work scope and schedules affected
- Design, development, and test effort involved
- Product documentation revision or replacement required
- Effects on warranty and other contractual considerations, delivered product (e.g., whether it requires recall, retrofit, replacement), spare/replacement parts, and environmental considerations
- Modifications required in manufacturing, assembly, installation, test, and operating or maintenance instructions

- Modifications required to training devices and training materials
- Effects on the performance or on the functional and physical interfaces with other products.

Another best practice is to institute a process to ensure that changes to a CI are complete and that the changes have not introduced any unanticipated issues. This is often part of a change verification process that includes verifying the consistency of the product, documentation, operation/maintenance information, interfaces, and training after change completion.

Configuration Status Accounting

Configuration status accounting is the function of reporting the current state of a system (or any configuration) efficiently, accurately, and quickly. The data for status accounting are a product of many systems—those used for project management, engineering, manufacturing, quality assurance, release, change control, logistic support organizations, and the customers. In an optimal CM system, these data are easily extracted, correlated, and maintained for status accounting in a database. Ideally, configuration status accounting data are a byproduct of these other systems. For example, in software configuration management, status accounting data are the result of baselining software versions, providing library control, and executing change management for software and its documentation.

For this CM function, configuration managers should implement two key best practices:

- Design configuration data and the CM database for integration with other systems in the enterprise, from finance to engineering, manufacturing, release management, and maintenance.
- Design CM data capture to provide visibility and traceability of the product configuration and the status of release of new product configuration information.

Configuration Verification and Audit

This CM function ensures, through formal functional and physical configuration audits, that a product's specified verification requirements—including tests, demonstrations, inspections, and analyses—have been met. The functional configuration audit (FCA) systematically compares requirements with the results of specified verifications. The physical configuration audit (PCA) determines whether the product is consistent with its design documentation.

This CM function also ensures that the content of the CM database is accurate. Operational systems must be validated periodically to ensure consistency between the in-use

product and its current baseline documentation. A critical function of this activity is verification of the incorporation of modifications.

The audit process has three phases: planning and preaudit preparation, execution of the configuration audit, and postaudit follow-up and closeout. Planning is as important as the audit itself. Planning is considered effective if

- audit requirements are consistent with the acquisition strategy and
- the audit schedule, or agenda, is keyed to program events and the availability of items, information, and personnel, resulting in
 - ❖ approved functional/allocated configuration documentation;
 - ❖ FCA prior to or concurrent with PCA, following CI/CSCI verification testing;
 - ❖ PCA conducted on an article in production (operational) configuration;
 - ❖ incremental hardware PCAs shadowing the assembly or test sequence; and
 - ❖ software PCA after integration testing.

The audit plan and agenda should address the following:

- Location and dates for each audit
- Composition of the audit team—government, contractor, subcontractor—and the team members' functions in the audit
- Identification of government, contractor, and subgroup chairpersons
- Documentation to be available for review
- Chronological schedule for conduct of the audit
- CIs/CSCIs to be audited and specific units to be audited
- Documentation to be audited and reference material
- Detailed information pertinent to the audit, for example, team requirements, facility requirements, administrative information, and security requirements.

Overall CM Best Practices

To summarize, PMs and configuration managers can ensure a successful CM program by applying the following best practices:

- Understand and use a comprehensive guide to CM, such as the DoD-adopted standard (EIA-649-B) and its handbook (GEIA-HB-649A) or MIL-HDBK-61A to implement CM. Both contain examples and tools for robust CM methods; for example, MIL-HDBK-61A has activity guides showing who does what for each CM function.
- Design metrics for the CM processes and build them into the CM system, including the supply chain.

- Plan for the business context and plan CM activities based on program milestones. This CM planning should begin with the request for proposals for the product.
- Train the CM staff and cross-train personnel in functions that integrate with CM; better understanding and integration from other functions are the secret to passing any audit. Trained personnel become resources for backup and for succession planning.
- Use a CM standard (for example, the principles in EIA-649-B) as an assessment tool for evaluation and troubleshooting.
- During incremental supplier configuration verification and audits, ensure that CM requirements flow down the supply chain.

¹Interim DoD Instruction 5000.02, “Operation of the Defense Acquisition System,” November 25, 2013.

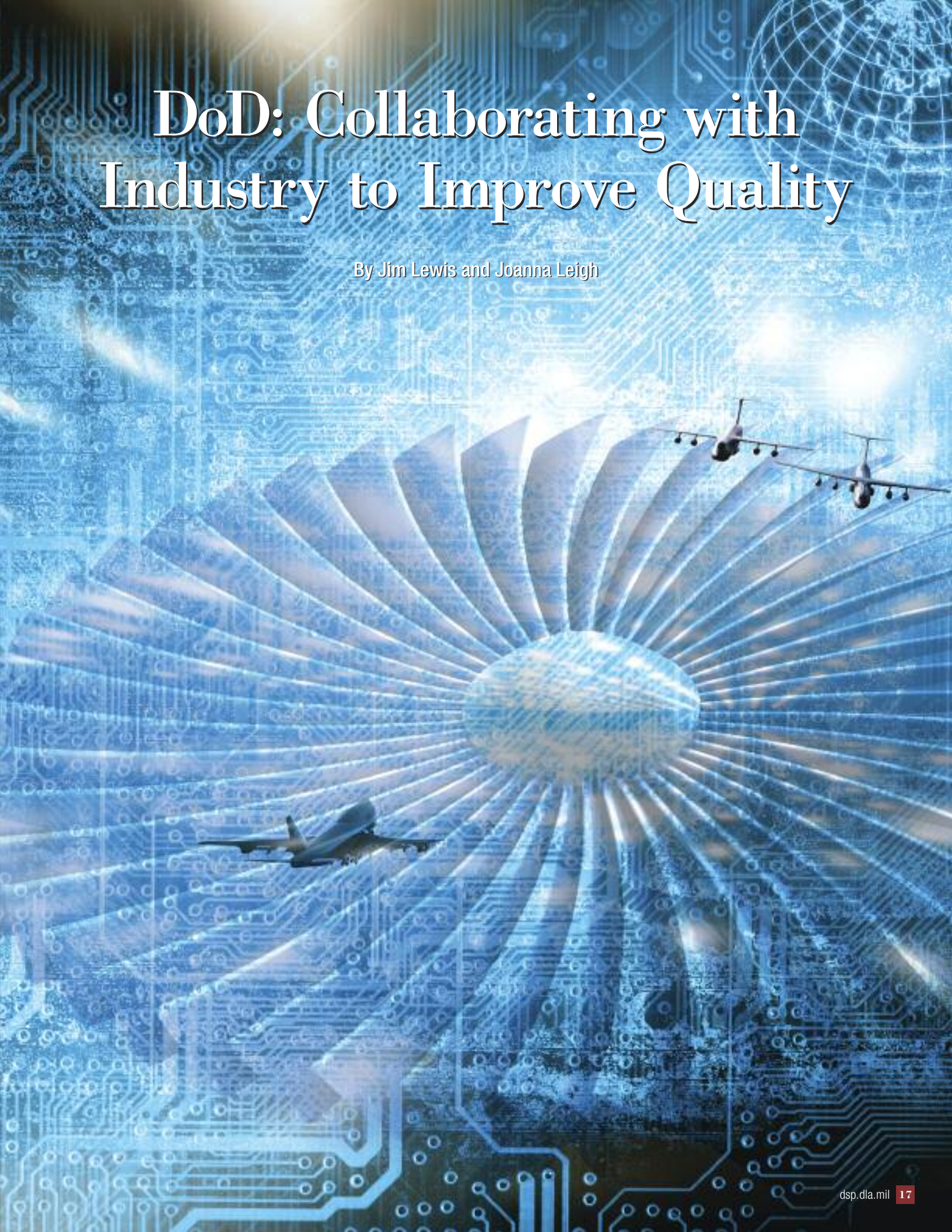
About the Authors

Denise Duncan is a senior fellow at LMI with 30 years of information systems management experience. She has managed a wide variety of projects, from assisting senior leaders with portfolio management to strategic planning for chief information officers. For the last 10 years, Ms. Duncan has worked extensively on the application of data management (DM) principles to engineering and scientific data. She has authored standards, handbooks, and training materials in enterprise-level DM and information management. Ms. Duncan has been honored as a technical fellow of TechAmerica and is the vice president for programs in the local chapter of Data Management Association—International.

Al Lager has been an industry spokesperson on military standards concerning CM, DM, and related topics since the early 1970s and has chaired working groups responsible for ANSI/EIA industry consensus standards for CM, DM, data interoperability, and exchange. Among other things, he served as the team leader and principal author of EIA-649, “National Consensus Standard for Configuration Management,” and principal editor of EIA-649-B; represented industry on DoD’s Configuration Management Advisory Group; authored MIL-HDBK-61 and 61A, *Configuration Management Guidance*; and served as industry team leader for EIA-836, “Configuration Management—Data Exchange and Interoperability.” ✨

DoD: Collaborating with Industry to Improve Quality

By Jim Lewis and Joanna Leigh



The Performance Review Institute (PRI) is a global provider of customer-focused solutions designed to improve process and product quality by adding value, reducing total cost, and promoting collaboration among stakeholders in industries where safety and quality are shared goals.

Created in 1990 by SAE International—known then as the Society of Automotive Engineers—PRI is a not-for-profit organization originally set up to administer Nadcap, the industry-managed special process and product accreditation program for the aerospace industry. Nadcap was developed by government and industry to continually improve quality while reducing costs.

Nadcap is now just one of the industry-managed programs administered by PRI with DoD involvement. The other is the qualified products list (QPL). Both programs involve representation from DoD at key levels of the decision-making process. A number of developments have occurred since the programs were last featured in this publication in 2005.

The PRI QPL Program

The purpose of the QPL program is to list manufacturers whose products have been certified by PRI as meeting specific standards. Certifications issued by PRI are for specific product designations and plant locations.

The need to maintain QPLs for critical specifications resulted from DoD's acquisition reform initiative, in particular, DoD's effort to transfer military standardization documents to non-government standards (NGSs). Military specifications that contained QPLs were a problem to convert because NGS organizations did not have a mechanism to manage QPLs.

In 1996, PRI, in coordination with DoD, undertook a pilot program for industry-managed QPLs. This pilot program, consisting of SAE International technical committee volunteers, culminated with guidelines, to be used by standards developing organizations (SDOs), for preparing mandatory qualification to requirements in standards and technical specifications. PRI launched its QPL program in 1998.

For many, the establishment and usage of PRI QPLs for industry standards have provided a vital mechanism to transfer QPLs associated with government standards that are converted to industry standards. Without this mechanism, there would be no way for industry standards to have industry QPLs. In the age of combining the resources of government and industry to share costs and standardize, the PRI QPLs are a necessary component. Government usage of industry standards would be severely crippled without the PRI QPLs.

Currently, 73 industry specifications require the use of PRI QPLs for critical aerospace products, such as fluid fittings, fluid hoses, elastomeric seals, sealants, and organic coatings, with several more being developed. These 73 specifications cover more than 67,000 qualified parts contained on the PRI QPLs. This is an increase of more than 100 percent since 2005, when there were 36 industry specifications requiring PRI QPLs.

The shared investment has the potential to significantly reduce qualification infrastructure costs for the supplier, industry, and government. As an example, for sealants, benefits have been realized by replacing government laboratory testing (which, in some cases, could take up to 9 months) with new observation and surveillance procedures. The new procedures have extended the shelf life of these materials from 3 months to 12 months, and they allow shipments to occur weekly. Savings of approximately \$300,000 per year can be attributed to this alone.

The PRI QPL organizational structure consists of technical qualified product groups (QPGs), which report directly to the Qualified Product Management Council (QPMC). The QPMC handles the strategic and tactical operations of the program. The QPGs, which comprise original equipment manufacturer (OEM) and government technical experts from SDO technical committees, are responsible for determining qualification requirements, developing operational program documents, reviewing and accepting test plans and test results, and making the final decision to list a company and product on the PRI QPL. Government representatives on the QPGs and QPMC come from the military services, the Defense Logistics Agency, and DSPO.

In 2013, the QPL program underwent a significant operational change, because much of the day-to-day activity is now conducted electronically. Since 2006, the QPL itself has been accessible online for procurement and quality purposes. Available in real time, from anywhere in the world with an Internet connection, the online QPL facilitates open communication between manufacturers and their customers and saves time sourcing compliant suppliers. In a further development, the entire process from applying to, to becoming listed on, the QPL transitioned from a paper-based process to an electronic one in 2013. As well as being more environmentally friendly, electronic submissions are processed quicker, which means that manufacturers get approved faster and the government and industry participants have better access to up-to-date data regarding compliant manufacturers. Other project-based activity was also made electronic, with QPG members now able to view project statuses and submit their disposition of a ballot of a project online, while QPMC members can now view project statuses for all product groups for their oversight of the program.

Nadcap

Nadcap is the leading worldwide cooperative program of major companies designed to manage a cost-effective consensus approach to special processes and products and provide continual improvement within the aerospace industry. The concept was initiated in a 1985 conference on government and industry as equal partners. The conference participants recommended a consensus solution to duplication of supplier quality assurance systems. Over the next several years, these entities worked closely together to define program operation details. The resulting program—Nadcap—was officially launched in 1990.

Specifications established by government, prime contractors, and industry are utilized when creating PRI audit criteria for each specific special process or product to ensure that procedural and compliance job audits are thorough and that customer requirements are being met. Nadcap special processes include nondestructive testing, heat treating, materials testing, chemical processing, coatings, welding, nonconventional machining, surface enhancement, and conventional machining. Nadcap special products include composites, electronics, fluid distribution systems, elastomeric seals, and sealants. In 2013, the number of Nadcap audits conducted globally was almost 5,000 across 52 countries, with the United States continuing to account for the majority of audits.

A few years ago, the organizational structure of Nadcap was streamlined to ensure it remained robust and considerate of government and industry representatives' time. Specifically, Nadcap's organizational structure was flattened to two levels: tactical (Nadcap Management Council) and technical (task groups). Strategy and policy are determined by the PRI Board of Directors, which is made up of representatives from industry. Government technical and quality experts feature throughout the Nadcap organizational structure to ensure DoD interests are adequately represented.

The Future

The PRI QPL program continues to expand, with interest being generated from committees involved with propulsion lubricants, greases, anti-icing and de-icing fluids, and fasteners. In 2012, the area of composites was established as being of significant interest to government and industry, with its own QPL requirements. The first composites standard was published, and the first applications to be listed on the QPL were submitted in 2013. They are currently going through the approval process. As new or revised specifications include the PRI QPL requirements, it is imperative that DoD and industry representatives work together to define the technical and qualification requirements for products that will meet the end-item performance requirements.

Continued government involvement in these programs is essential because the transition from military specifications to NGSs carries responsibilities. To ensure that military

requirements continue to be supported, DoD engineers must participate with the various committees engaged in updating NGSs. They must be willing to contribute to the constant maintenance and improvement of the standards. DoD engineers must be willing to carry their fair share of the standardization workload along with their industry and academic counterparts.

Nadcap is dynamic and is driven by government and industry needs. Any source can suggest that new task groups be established. A value assessment is then undertaken to determine government and industry interest. With enough interest, technical experts are assigned to develop the audit criteria and to define auditor qualifications. The most recent task group is Measurement and Inspection, intended to provide adequate systemic and detailed auditing capability dedicated to the means, people, methods, and all other conditions required to be fulfilled in order to control the “geometric inspection process.” Dimensional measurement of components is routinely used throughout industry to verify the conformance of the manufactured product to the specification. To ensure measurements are reliable, the measurement capability must be suitable for the feature being measured. The scope of accreditation covers dimensional measurement and inspection as it relates to calibration and units, product definition, inspection planning, equipment validation, asset care of equipment, environmental control, competencies, and compliance.

Another area under development is metallic materials manufacturing, which covers casting, forging, and raw material manufacturing. In common with other Nadcap accreditation areas, it is expected to help reduce scrap, rework, and lead-time; contribute to better end product manufacture; reduce overall cost for the industry; and improve the manufacturing process.

Existing task groups urge continual improvements with timely revisions to operating procedures, audit criteria, and standards to meet the goals of reducing risk and improving supplier responsiveness.

Conclusion

Both the PRI QPL program and Nadcap are used by OEMs and government agencies in their supplier management structure (supplier quality, purchaser quality, and user surveillance). They can be viewed as integral supplements using industry standards, procedures, oversight, and core values. Both rely on industry/government teaming and are technically driven with the same goal of excellent quality. As an association, PRI is committed to providing industry and government a unique and unbiased forum so that meetings and results focus on quality and safety. However, the responsibility of the users (government agencies and prime contractors) does not shift with the utilization of these industry-managed programs.

In the course of daily operations, if you hear the PRI QPL program or Nadcap mentioned, know that DoD is represented at all levels of these two industry-managed programs. By visiting the PRI website (www.p-r-i.org), you can learn more about the industry-managed programs managed by PRI and find key points of contact at DoD. If you have questions about program operations, technical requirements, or quality requirements, or if you want to become more involved, please contact PRI at 724-772-1616.

About the Authors

Jim Lewis is a program manager at PRI responsible for the QPL program, as well as for coatings, elastomer seals, fluid distribution systems, materials testing, and sealants. Having spent much of his career in industry, Mr. Lewis now works closely with both government and industry representatives to optimize both the Nadcap and QPL programs to meet their needs.

Joanna Leigh is PRI's marketing manager, responsible for all marketing and communications activities globally. She works to ensure that the Nadcap brand remains consistent with emphasis on continual improvement within regional sectors and, in particular, with the Nadcap Supplier Support Committee to help manufacturers around the world embrace best practices for improved quality. ✨

Better Training for Better Defense

Using Personnel Credentialing Standards and Conformity Assessment to Improve National Security

By Vijay Krishna



In today's environment of new and emerging security threats, private-sector standards and conformity assessment have become hugely important strategic tools for increasing defense preparedness and national security. DoD and NATO policies for standardization emphasize adopting suitable private-sector standards whenever possible and advantageous, rather than developing military standards. Standards set benchmarks for quality and performance that help protect the public interest and safe use of products and processes. From the 9-11 Commission's endorsement of an American National Standard (ANS) for disaster and emergency management, to the Consumer Product Safety Improvement Act of 2008, which mandates compliance with ANSs for all-terrain vehicles and toy safety, the increase in government reliance on voluntary consensus standards has been sizable.

While DoD continues to support and use several civilian standards in traditional domains, such as weapons systems, design and manufacturing, procurement, delivery, and logistics, standards are now becoming critical in newer technology domains as well, such as networks, data transfers, Internet protocols, video formats, cloud computing, software development, and biometrics. However, the technologies that govern these areas are extremely dynamic and require an adaptive standards and conformity assessment framework.

Historically, in a primary-products economy, standards were developed to ensure product safety and to facilitate the movement of goods across borders. The industrialized era saw the creation of a number of process standards, such as quality management systems, to ensure that these products were produced and operated in a safe environment. In the current knowledge economy, however, people have become the most critical resource for an organization. Trained, qualified, and competent personnel are an entity's lifeblood. An organization's tomorrow depends on the knowledge, insight, foresight, and competence of today's employees.

In tune with these trends, the last decade has seen the creation of standards related to the training, education, assessment, and credentialing of people. The term "credential" is an umbrella term that includes degrees, diplomas, licenses, certificates, badges, and certifications. A credential is a marker to show competence for job skills and knowledge. It helps the employer make informed hiring decisions and ensures that only an individual with demonstrated competence is allowed to practice in a particular profession. If credentials are awarded to unqualified individuals, the public safety of Americans and the integrity of our national defense system could be compromised.

The increased demand for certified professionals has also led to the proliferation of training and certification bodies. However, employers are often unsure of the quality and reliability of these organizations, as well as of the competencies (if any) being communi-

cated through their credentials. Many credentials are self-declared and do not provide the skills and competencies needed by employers. A critical element lacking in many training programs is a valid assessment to measure intended learning outcomes. Fortunately, these problems can be addressed with standards that identify a process for developing competencies, curriculum, validation, and assessment for certification programs. These standards provide the framework for aligning learning systems and validation by an independent third party, such as the American National Standards Institute (ANSI).

Arguably, the biggest security threat confronting the United States relates to cybersecurity. Former Secretary of Defense Leon E. Panetta has warned that the United States is facing the possibility of a “cyber-Pearl Harbor” that could dismantle the nation’s grid, transportation system, financial networks, and government. Most security experts believe that cybersecurity is not just a technology problem, but one that requires dealing with both technology and the human side of the equation. According to Ronald Heifetz and Marty Linsky of Harvard University, the most common source of leadership failure by people in positions of authority is to treat adaptive challenges like technical problems.

Cybersecurity is not just a problem of security systems but a challenge to our mindset of invulnerability. Organizations must ensure that they have not only secure systems, but also an adequately trained and competent cybersecurity workforce to manage them. Standards and conformity assessment can play an important role in establishing requirements to assess the quality of training and competence of individuals. Personnel certification based on appropriate skill standards provides further assurance not only that individuals have met the required competencies, but also that an independent third party has verified compliance to the standard to provide quality assurance.

Standard for the Certification of Personnel

To train and maintain a world-class cybersecurity workforce ready to take on the digital battlefield, DoD developed 8570.01-M, *Information Assurance Workforce Improvement Program*. The manual addresses the credentialing and continuing education of all DoD employees with privileged access to DoD information systems. Under this directive, the certification body must demonstrate compliance to ANSI/ISO/IEC 17024, “Conformity assessment—General requirements for bodies operating certification of persons,” which was developed by ISO and later adopted as an ANS. This standard was based on the need for public protection by establishing that individuals have the required competencies to perform their job. Several U.S. federal agencies have recognized the standards as a critical requirement for personnel certification bodies that offer certification in areas related to public health, environment, and national security. The standard, originally published in 2003 and revised in 2012, has already affected the delivery of quality certifications worldwide.

Why should a certification body be required to meet a national/international standard? What are the potential benefits of an accredited certification for various stakeholder groups? The standard uses several principles to provide a benchmark for offering quality personnel certification programs, building confidence in the competence of professionals in a wide spectrum of industries.

Certification refers to the process through which a nongovernmental entity grants time-limited recognition to an individual after verifying that he or she has met established criteria for proficiency or competency, usually through an eligibility application and assessment. Certification programs that follow ANSI/ISO/IEC 17024 must meet the following requirements:

- *Credibility.* The certification examination must be fair, valid, and reliable. A valid test correctly measures whether an individual has the necessary competencies for the job. Validity is an indicator to establish that the process measures what it is intended to measure, whereas reliability shows that the test measures a person's abilities in a consistent manner. The standard not only requires assessment for initial certification but also assessment of continued competence through a recertification process.
- *Impartiality.* The certification body should have structure, policies, and procedures that ensure impartiality and objectivity and manage conflict of interest arising from certification activities.
- *Independence.* The certification functions should be independent of training to ensure that confidentiality, information security, and impartiality are not compromised.
- *Transparency.* The certification body must have an active complaints process to resolve complaints against its activities, as well as complaints against individuals that it has certified.
- *Accountability.* The certification body should have a due process for taking away the credential for unethical or incompetent behavior.
- *Balanced representation of stakeholders.* The certification body should involve key stakeholders in making certification-related decisions. In addition, subject matter experts should be involved in creating the certification scheme requirement based on a valid job or practice analysis.
- *Other requirements.* The standard is very comprehensive and covers all aspects of certification, including test security, recertification, resource requirements, confidentiality, competence of personnel involved with the certification activities, financial requirements, and use of certificates and logo marks. Further, the certification body should develop a management system for continual improvement of its certification program.

Standard for Training Certificates

The last few years have seen an extraordinary growth in training certificates. According to the Center on Education and the Workforce at Georgetown University, certificates have been the fastest growing post-secondary credentials awarded over the past several decades. According to the Integrated Postsecondary Education Data System, more than a million certificates were awarded in 2010, up from 300,000 in 1994. Every year, millions of dollars are spent training employees, through both in-house and commercial training programs. Unfortunately, a lot investment in training is wasted by sending employees to attend training programs that do not provide any skill enhancement. ASTM International developed the ANS ASTM E2659-09, “Standard Practice for Certificate Programs,” in response to growing concerns relating to the quality of training programs. The standard details a framework to provide high-quality, competency-based training and educational programs, and it requires that programs meet predefined industry requirements for content, employ a criterion-referenced examination, and include a mechanism for continual feedback for quality improvement. ASTM E2659 has the following main requirements:

- *Validated competencies.* Competencies are the foundational building blocks in developing a training program and should be derived from a process that is formally structured and empirically based. The process should involve full participation from the industry, employers, and subject matter experts.
- *Learning process.* The instructional delivery must include appropriate instructional design and must be flexible to meet the needs of the individual learner.
- *Learning outcomes assessment.* Assessment is the process of measuring an individual’s competencies to perform a required job. The standard requires a criterion-referenced examination to measure intended learning outcomes.
- *Continuous improvement process.* The standard requires the training provider to institute an ongoing systematic process to ensure that the training curriculum is updated and remains market relevant as skill sets change. Quality improvement processes should be embedded throughout the training program.

The U.S. Army Combat Readiness/Safety Center has taken a lead in using ASTM E2659 in delivering high-quality training courses in several areas related to safety. This is an important initiative to enhance technical and managerial competencies for personnel working in explosive safety, ground safety, and aviation safety. Use of accredited training and certification also helps military service members demonstrate to civilian employers that training and skills attained in the military are on par with those gained through traditional civilian pathways. Thus, credentialing can also be an incentive for soldiers to stay in the military.

ANSI Personnel Credentialing Accreditation Programs

ANSI administers accreditation programs based on ANSI/ISO/IEC 17024 for personnel certification bodies and on ASTM E2659 for training organizations. The ANSI accreditation process itself is based on ISO/IEC 17011, “Conformity assessment—General requirements for accreditation bodies accrediting conformity assessment bodies.” ISO/IEC 17011 is extremely rigorous and ensures that only those organizations that meet the stringent requirements under the standard are accredited. An independent, third-party accreditation is an “accountability mechanism” to ensure the quality and legitimacy of organizations offering credentials. If a consumer sees the ANSI accreditation mark on a credentialing body’s certificate, he or she can be confident that the body has the structure and processes in place to offer a valid credential. It also signals to the employer that the credential holder has undergone a valid assessment to verify that he or she has the necessary competencies for a position. To date, ANSI has accredited 52 organizations for 175 certification programs and 29 training providers across a range of industry sectors involving more than 5 million workers.

DoD has a long history of reliance on non-government standards for products and processes, and today, DoD is a leader in using national and international standards for credentialing individuals. In view of the growing threat of cyberwarfare, DoD is committed to maintaining an unrivaled, globally competitive cybersecurity workforce by using standards, training, and certifications for its workforce. DoD 8570 highlights the growing importance that the agency puts on the capabilities and competence of those working in the mission-critical areas of information assurance. The use of standards helps build confidence in the people working to maintain national security. In a rapidly changing working environment with both new technologies and emergent threats, acquiring new skills and capabilities is a constant requirement for armed forces personnel. With confidence in the people at the helm of national security, we can be assured of our protection against the threats, whether digital or physical, that face our nation.

About the Author

Vijay Krishna is the director of ANSI’s personnel credentialing accreditation programs. In this position, Dr. Krishna is responsible for the overall management of ANSI’s personnel certification accreditation program based on ANSI/ISO/IEC 17024 and the certificate accreditation program based on ASTM E2659 standards. He is a recognized expert in the field of personnel credentialing and works closely with various national and international agencies that are involved in developing competency-based credentialing systems. ✨

Anticounterfeit Best Practices

By Taylor Wilkerson and Joe Doyle

Counterfeit parts are a real threat to mission effectiveness and data assurance, as these three examples demonstrate:

A pilot takes off to complete an important mission. As the aircraft ascends, warning lights indicate an engine failure. The pilot has to scrub the mission and return to the airfield. The next day, maintenance crews find the failed part: an essential piece of the engine. Upon further investigation, they find that the part is a counterfeit made from an alloy that is less expensive than the specified alloy.

A team of soldiers are on patrol. Suddenly, a piece of communications equipment starts to overheat and needs to be shut down. The team must return to base with limited communication capability. An inspection reveals that a counterfeit battery is to blame.

A combatant command planning team is drafting response plans to an area with increasing political tension. The plans detail force strength, deployment, and tactical facets of the response. As the team sends the plans to the commander for review, a counterfeit network switch sends a copy of the plans to an offshore IP address, giving information to an entity potentially seeking ways to sabotage our response.

Whether trying to gain some economic advantages or to deliberately compromise equipment, counterfeiters will always have an incentive to get their products into legitimate supply chains. The good news is that you can reduce the risk of counterfeits entering your supply chain by adopting proven leading practices. What we provide here is an overview of anticounterfeit best practices.

About Counterfeits

“COUNTERFEIT” DEFINED

To set the stage, let's start with a definition of “counterfeit.” From a legal standpoint, the term tends to refer to items that infringe on a trademark or copyright. This definition works well for most commercial items when the primary interest is protecting the trademark or copyright holder from having cheap knock-offs of its product on the market. For most DoD applications, however, we are not as concerned about the trademark protection (although that can be important for DoD suppliers) as we are about the proper form, fit, and function of the item. For this reason, DoD defines a “counterfeit” as follows:


- (1) An unauthorized copy or substitute part that has been identified, marked, and/or altered by a source other than the part's legally authorized source and has been misrepresented to be from a legally authorized source;
- (2) An item misrepresented to be an authorized item of the legally authorized source; or
- (3) A new, used, outdated, or expired item from a legally authorized source that is

misrepresented by any source to the end-user as meeting the performance requirements for the intended use.¹

In other words, a counterfeit is an item that is represented as something other than what it is. It is important to note that poor quality and other supply chain issues, such as late or incomplete shipments or the wrong item shipped, are not considered counterfeits.

SOURCES OF COUNTERFEITS

Economic actors and intentional actors are the two primary sources of counterfeit items. The two sources differ in their motivation. Economic actors—the most common source of counterfeits—are motivated by the potential for large profits possible in making substandard items and selling them as brand-name items. Economic actors may also insert compromised electronics components into the market with the hope of collecting personal information for the purpose of fraud or identify theft. Economic actors tend to target broad markets rather than specific customers, and their intent is not necessarily to harm the customer other than economically. Intentional actors, which often are state sponsored, are motivated by the ability to sabotage or weaken an adversary’s capability by inserting substandard or compromised parts into the supply chain. The largest current threat from intentional actors is thought to be the insertion of compromised electronics and communications items into a network or system, with the goal of extracting sensitive data. Intentional actors tend to have a specific target in mind.



The largest current threat from intentional actors is thought to be the insertion of compromised electronics and communications items into a network or system, with the goal of extracting sensitive data.

COSTS OF COUNTERFEITS

Counterfeit parts come with real costs—both financial and operational. The financial costs are related to receiving counterfeit items and include such things as the costs of replacing the counterfeit items with legitimate items and the inventory management costs of handling and pulling suspected counterfeits out of inventory. That, in turn, can result in stock-outs of legitimate items needed to keep a system or piece of equipment operational, impeding operations. Another operational cost concerns the negative impact on

the operations of systems and equipment—and the safety of our warfighters—if a counterfeit item is installed. The sooner the counterfeits are detected and removed, the less work is needed to mitigate the problem.

Scoping the Problem

There is no doubt that counterfeit parts can and do present a significant threat to readiness and budgets. The question is, what can you do about it? The answer is to use a risk management approach to protect yourself against counterfeits and to rapidly respond when counterfeits are discovered. We recommend a risk-based approach because counterfeits are a risk to operations. Risk management practices are designed to manage uncertainty, with a focus on preventing actions that could increase costs or disrupt operations. That is why risk management approaches are ideal for managing the uncertainty and operational threats that come with counterfeits.

The first step in managing counterfeits is to cut the problem down to a manageable scope. It is natural to want to prevent counterfeit parts from affecting any item in your supply chain. However, most organizations are managing thousands of parts from hundreds of suppliers (each with their own hundreds of suppliers and so on). Therefore, documenting and managing that scope of operations are nearly impossible. So start your process with a good look at what counterfeit risks you should be most worried about. Which items handle sensitive data? Which ones can cause a risk to life or the mission if they fail? Which items are difficult to procure? Essentially, what is your risk—financial or operational—if a counterfeit of that item gets in your supply chain?

The second step is identifying where you have risks for counterfeit items entering the supply chain. This can include where you or your supplier rely on open market purchases or have experienced counterfeit events. This requires an understanding of where counterfeits can enter your supply chain, such as through

- unauthorized distributors, especially those known for selling refurbished or reclaimed items;
- facilities located in countries or regions known to be significant sources of counterfeits; and
- facilities or transportation routes with poor security or access controls.

The intersection of parts that have a high impact if they are counterfeit and those with a high opportunity for counterfeiting is where you should start. Your goal should be to reduce the risk of counterfeits to the extent your resources will allow. Because it is nearly impossible to directly manage your entire supply chain, and because counterfeiters are always pursuing new methods to get counterfeits into legitimate markets, it is nearly impossible to eliminate the risk of counterfeits. But, by prioritizing attention on the parts

and supply chain processes that represent the most significant risk, you can greatly reduce your risk exposure through some leading counterfeit management practices.

Reducing the Risk

Once you know which parts you want to start with, you can begin your risk management activities. We use a risk management approach for counterfeits because risk management tools are designed to manage the uncertain and dynamic threats to the supply chain, which counterfeits certainly represent. Risk management approaches also recognize that resources need to be prioritized to address the greatest threats (with methods for ranking threats) combined with plans to quickly respond and recover when risk events occur, in this case, when counterfeits are discovered in the supply chain.

SUPPLY CHAIN VISIBILITY AND INTELLIGENCE

Proactively managing risk requires knowledge and visibility of the supply chain. Start with mapping your supply chain for the selected parts with as much information as you have. Often, using a framework like the Supply Chain Operations Reference model will help with this, as will a supply chain mapping tool. In the mapping tool, you should be able to identify where each location is geographically and what activities take place there (what components are manufactured, what other products are made there, and so on). Keep in mind that the address on file for most companies is not the manufacturing location and that many manufacturers outsource production of some items. From this mapping, identify where counterfeits can enter the supply chain and where you do not have enough information to judge the risk of counterfeits.

In mapping the supply chain, you should capture, to the extent possible, information that will help you understand where counterfeit risks lie. Essentially, you want to look for places where there is an opportunity to insert counterfeit items into the supply chain. Keep in mind that economic and intentional actors use different methods to insert items. Economic actors look for grey markets or even black markets where they can sell their products regardless of the customer. Intentional actors, on the other hand, look for weaknesses in specific supply chains that may enable them to get their counterfeit into the hands of their target user.

Capturing all of this information requires some element of supply chain intelligence. You should look for information on the following business practices:

- *Procurement.* Do the organizations in the supply chain follow good practices to ensure their suppliers deliver authorized products and take appropriate actions to secure their facilities and supply chain?
- *Personnel security.* Do the organizations in the supply chain follow employee back-

ground check procedures and other character vetting as appropriate for the type of product being handled?

- *Physical security.* Do the facilities in the supply chain have appropriate physical security, including access controls and monitoring to prevent unauthorized access to the facility or to secured areas?
- *Transportation security.* Do the organizations in the supply chain use appropriate transportation security to ensure that products are not tampered with or diverted while in transit?

The specific levels of security you are looking for in each area will depend on the product and the potential opportunities for counterfeit insertion. For example, if your concern is intentional actors, you may need to focus on personnel security and transportation security. On the other hand, if your concern is economic actors, you may need to focus on procurement actions.

SUPPLIER RELATIONSHIP MANAGEMENT

At this point, you should have a good idea of the areas of concern in your supply chain. The next step is to take actions to reduce the risk. Most actions concern either supplier relationships or technological solutions.

Supplier relationships involve working with your suppliers to reduce or eliminate the counterfeit threat. One option is to simply stop doing business with suppliers that present a counterfeit risk and to work only with trusted suppliers. This works well for environments where there are several suppliers for the product and procurement rules allow for disqualifying suppliers based on factors such as insufficient security.

If you have limited flexibility in selecting suppliers, you can work with them to improve their counterfeit prevention practices. Working with suppliers can take many forms. Perhaps one of the simplest actions to take is to require suppliers to adhere to a security or counterfeit prevention standard. For example, ISO 28000, “Specifications for Security Management Systems in the Supply Chain,” covers good practices for supply chain security. For a more hands-on approach, you can collaborate with suppliers to review their counterfeit prevention practices and help them improve their security. The approach you take should consider the amount of risk the supplier represents and the resources you have to apply to reduce the risk. When there is a single supplier for a product, collaborating with that supplier to reduce the risk may be the best option for reducing risk while ensuring product availability.

PRODUCT PROVENANCE

In most transactions, knowing the entity from which you are buying a product is clearly

a best practice for avoiding becoming a victim. Where possible, purchase directly from a trusted source that actually manufactures the item and that places an identifier—often termed an “authentication” mark—on the item during manufacture.

Buying directly from the manufacturer is not always possible. DoD, for example, often operates and maintains weapons systems long after the original component manufacturer (OCM) ceases production. In those cases, documenting product provenance may be the next-best practice. “Provenance” is the chronology of the ownership, custody, or location of an object. Normally, the primary purpose of tracing the provenance of an object or entity is to provide contextual and circumstantial evidence for its original production.

DoD has long required traceability back to the OCM for many of its high-risk commodities. Paper trails, however, are not difficult to falsify. There are many documented instances in which authentic-looking chain-of-custody paperwork accompanies counterfeit material. We need a more reliable method to establish authenticity or provenance.

Several commercial firms offer tools for authenticating or verifying a component’s provenance. Below are four of the more innovative tools:

- *Ceramic taggant technology.* We can apply ceramic taggants during manufacture or later. Providers proclaim that their technology is physically and chemically robust and applicable to a wide variety of commodities. They can program proprietary spectral algorithms into handheld readers. This allows minimally trained users in the field to recognize preselected characteristics and thereby confirm authenticity or provenance of properly marked items.
- *Laser marking.* We can accomplish laser marking by the manufacturer or others later in the supply chain. Providers offer processes that engrave an encoded mark into the surface of a broad range of commodities. These etchings provide for traceability and guarantee authenticity of the item. Their component profiles ensure protection of critical characteristics and allow reading the laser marking at any point in the supply chain.
- *Botanically generated DNA.* We can apply botanically derived DNA marks during manufacture or further down the supply chain. Providers attest that they can embed custom DNA sequences into a wide range of host carriers, including ink, varnish, thread, laminates, and metal coatings. Supply chains can detect the presence of these DNA markers in the field and send suspect items to a laboratory for more sophisticated forensic-level analysis.
- *Physical unclonable function (PUF).* A PUF is a physical entity that is embodied in a physical structure. PUFs can be applied to numerous commodity types. Supply chain personnel can use off-the-shelf devices to detect PUFs, as well as authenticate the product in the field, in a matter of seconds.

Many other tools for authenticating or verifying provenance are emerging. The challenge is to select secure counterfeit avoidance measures that do not complicate either the manufacturing or supply chain processes. Detection should also be relatively simple, fast, and field capable without being cost-prohibitive.

EDUCATION AND TRAINING

Combining supply chain visibility and intelligence with supplier relationships and product tracking technology can help secure the supply chain against counterfeits. However, remember that it is your personnel who must carry out the supplier relationship actions and use the tracking technologies. Therefore, a comprehensive counterfeit prevention program needs to include education and training for employees. The training should help employees understand the importance of preventing counterfeits and their specific role in counterfeit prevention. Through proper training, you can ensure that counterfeit prevention procedures and technologies will be properly applied throughout the supply chain.

Response and Recovery

Counterfeit management does not stop with prevention. Counterfeiters are motivated and persistent. You need to be prepared for counterfeits appearing in your supply chain despite your best efforts. You need a response and recovery plan for discovering counterfeits in your supply chain. When a suspected counterfeit item is identified, it—along with others in that shipment or with the same lot number—should be quarantined until the authenticity of the product can be verified. If the product is verified as counterfeit, you need to identify the source and work with any supply chain partners involved. Quarantining items may involve identifying instances in which a suspect item has been installed on a piece of equipment. In this case, your response procedures need to include processes for recalling that equipment into maintenance to remove the suspect part.

But removing the counterfeit items is only part of the process. You now have lost inventory that was intended to fill a future customer demand. Your response plan should include procedures to expedite the delivery of replacement inventory from a trusted and verifiable source. The faster you are able to respond to the counterfeit item, the less likely it is that you will see an interruption in service to your customers.

Conclusion

Counterfeit parts are a reality that can put operations at risk. However, you can take many steps to reduce the risk of counterfeits entering your supply chain. Often, a first

thought is to simply require suppliers to take action to prevent counterfeits. However, putting the onus on suppliers does not eliminate the risk of counterfeits. True prevention requires you to understand where the risks are and to take actions, in coordination with your suppliers, to secure the supply chain. Supply chain visibility and security procedures, together with product provenance technologies, can greatly reduce your risk exposure. But remember that no security method is 100 percent effective; include response and recovery processes in your counterfeit prevention plans.

The bottom line? Counterfeiters are resourceful and persistent. You will have to be equally resourceful and persistently vigilant in preventing counterfeits and quickly taking steps to eliminate any counterfeits that get into the supply chain.

¹“Detection and Avoidance of Counterfeit Electronic Parts,” *Defense Federal Acquisition Regulation Supplement*, DFARS Case 2012-D055, <https://www.federalregister.gov/articles/2013/05/16/2013-11400/defense-federal-acquisition-regulation-supplement-detection-and-avoidance-of-counterfeit-electronic>.

About the Authors

Taylor Wilkerson is a program manager in LMI’s Supply Chain Management program. He also co-chairs the Supply Chain Risk Leadership Council and is a co-lead of the Supply Chain Council’s Risk Management project team. Mr. Wilkerson is active in government and industry supply chain risk management discussions and is a contributing author to *X-SCM: The New Science of X-treme Supply Chain Management*. In addition, he is a senior fellow and adjunct professor with the University of Maryland R. H. Smith School of Business Supply Chain Management Center.

Joe Doyle is a retired submarine officer and a senior consultant at LMI. He manages a variety of research and development initiatives for the Defense Logistics Agency’s Weapon System Sustainment Program and similar tasks for other federal agencies. A certified Project Management Professional and Certified Manager, Dr. Doyle actively participates in academic, government, and industry anticounterfeiting efforts. ✨

Program News

Topical Information on Standardization Programs

OMB Releases a Request for Comments on a Proposed Revision of OMB Circular A-119

On February 12, 2014, the Office of Management and Budget (OMB) released a request for comments on OMB Circular A-119, “Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.” The circular is being updated to address changes that have taken place in the areas of regulation, standards, and conformity assessment since the circular was last revised in 1998. Though the comment period closed on May 12, 2014, the initial notice, which appeared in the Federal Register, is provided below for informative purposes only.

ACTION: Notice of Availability and Request for Comments.

SUMMARY: The Office of Management and Budget (OMB) requests comments on proposed revisions to Circular A-119, “Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities” (hereinafter, Circular A-119, or, the Circular) in light of changes that have taken place in the world of regulation, standards, and conformity assessment since the Circular was last revised in 1998. These materials are available at http://www.whitehouse.gov/omb/inforeg_infopoltech.

The National Technology Transfer and Advancement Act of 1995 (Pub. L. 104-113; hereinafter known as the NTTAA) codified pre-existing policies on the development and use of voluntary consensus standards in Circular A-119, established additional reporting requirements for agencies, and authorized the National Institute of Standards and Technology (NIST) to coordinate conformity assessment activities. In response, OMB in 1998 issued a revised version of Circular A-119, which remains the current version.

In this notice, OMB is seeking public comment on proposed revisions to the Circular. These proposed revisions reflect the experience gained by U.S. agencies in



Program News

implementing the Circular since 1998; domestic and international developments in regulatory, standards, and conformity assessment policy; concluding and implementing U.S. trade agreements; and comments received in response to OMB's March 2012 Request for Information on whether and how to supplement Circular A-119.

The proposed revision to Circular A-119 includes the following elements:

Preference for voluntary consensus standards. The revised Circular would maintain a strong preference for using voluntary consensus standards in Federal regulation and procurement. It would also acknowledge, however, that there may be some standards not developed using a consensus-driven process that are in use in the market—particularly in the information technology space—and that may be relevant (and necessary) in meeting agency missions and priorities.

Guidance on use of standards and participation in standards development. The revised Circular would provide more detailed guidance on how Federal representatives should participate in standards development activities. It would also strengthen the role of agency Standards Executives, encourage better internal coordination and training on standards, and update the provisions on how the U.S. Government manages and reports on the development and use of standards. The Circular would also provide criteria for agencies to consider when examining whether a standard meets agency needs and should be adopted.

Guidance on conformity assessment. The revised Circular would encourage agencies to consider international conformity assessment schemes and private sector conformity assessment activities in lieu of conformity assessment activities or schemes developed or carried out by the government, and set out criteria for agencies to consider when they are selecting or designing an appropriate conformity assessment procedure.

Enhanced transparency. The proposed revisions would provide guidance to agencies on how they should discuss implementation of the Circular in their rulemakings

and guidance documents; encourage agencies to alert the public when considering whether to participate in standards development activities; and set out factors for agencies to consider when incorporating standards by reference in regulation.

Burden reduction. The proposed revisions would require agencies to utilize the retrospective review mechanism set out in Executive Orders 13563 and 13610 to implement the Circular, including ensuring that standards incorporated by reference in regulation are updated on a timely basis. The revisions also encourage agencies to work together to reference the same version of a standard in regulation and procurements and coordinate on conformity assessment requirements, where feasible.

International considerations. The proposed revisions incorporate references to trade-related statutory obligations on standards-related measures and direct Federal agencies to consult with USTR on how to comply with international obligations with regard to standards and conformity assessment. They provide guidance on how to identify such obligations, direct agencies to take into account their obligations under Executive Order 13609 when they engage in standards and conformity assessment activities, and encourage greater coordination with respect to the Government's formulation of global strategies on standards, regulation, and international trade.

Events

Upcoming Events and Information

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.”

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 sup-



Events

Upcoming Events and Information

ported 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.dmsmsmeeting.com.



People

People in the Standardization Community

Welcome

Michael Harbaugh recently assumed the position of Departmental Standardization Officer (DepSO) for the National Geospatial-Intelligence Agency (NGA). Mr. Harbaugh started his career in 1983 as a cartographer with the Defense Mapping Agency (DMA), which subsequently became part of NGA. In 1995, he was assigned to NGA's Architecture and Standards Office, where he served as a standardization officer. Over the years Mr. Harbaugh has worked in a number of national and international forums, such as NATO's Joint Geospatial Standards Working Group where he currently serves as the U.S. Head of Delegation. We welcome him to this new role.

Farewell

Daniel Gleason, NGA DepSO, retired on July 24, 2014, after 35 years of federal service. Mr. Gleason began working at DMA as a nautical cartographer in 1979. He began writing hydrographic product specifications in 1986. Mr. Gleason was appointed to serve as the DSP manager for the National Imagery and Mapping Agency (NIMA) when it was established in 1996 from several predecessor organizations, including DMA. NIMA was renamed NGA in 2004. In addition to his DSP duties, Mr. Gleason was the geospatial intelligence portrayal standards manager at the National Center for Geospatial Intelligence Standards; the chairman of the Geospatial Intelligence Standards Working Group's Portrayal Focus Group; and the portrayal thematic coordinator and, later, the portrayal technical panel chairman for the Defence Geospatial Information Working Group, an association of military mapping organizations that is chartered to develop geospatial standards for NATO. We wish him well in retirement.

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.



communication



navigation

collaboration

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
April/June 2014	Standardization Stars
July/September 2014	DMSMS

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.



