

Defense Standardization Program

Journal

January/March 2007



DoD IT Standardization

Governance of IT Standards
Finding the Right Standards
The SDO/SSO Collaboration Tool



4



8

1 Director's Forum

4 "Openness"

An Important Principle for the Stewardship of DoD IT Standards

8 DoD IT Standards Program Strategy and Principles

Enabling Warfighters at Internet Speed

14 Governance of IT Standards

20 Finding the Right Standards

26 A Behind-the-Scenes Look at Managing DoD/Joint Interoperability

30 Collaborating with External Organizations to Develop and Set IT Standards

34 DoD Representatives to Organizations for IT Standards

38 DoD IT Standards Registry

44 The SDO/SSO Collaboration Tool

56 Harvesting

Creating an ISO Standard from a Military Specification

60 Lessons Learned in IT Standards Development

Departments

70 **Events** 72 **People**

Gregory E. Saunders

Director, Defense Standardization Program Office

Timothy P. Koczanski

Editor, Defense Standardization Program Journal

Defense Standardization Program Office

8725 John J. Kingman Road

Stop 6233

Fort Belvoir, VA 22060-6221

703-767-6870

Fax 703-767-6876

dsp.dla.mil

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*, J-307, Defense Standardization Program Office, 8725 John J. Kingman Road, Stop 6233, Fort Belvoir, VA 22060-6221. DSPO is not responsible for unsolicited materials. Materials can be submitted digitally by the following means:

e-mail to DSP-Editor@dlm.mil

floppy disk (Windows format) to *DSP Journal* at the above address.

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

For a subscription to the *DSP Journal*, go to dsp.dla.mil/newsletters/subscribe.asp



In this issue of the *Defense Standardization Program Journal*, we are focusing on information technology (IT) standardization efforts and initiatives underway at the Defense Information Systems Agency (DISA). DISA is the DoD Executive Agent for IT Standards. It is my pleasure to turn over my column in this issue to Mr. Mike O'Connor, Chief of the Interface Standards Division in the DISA Engineering Organization. Mr. O'Connor has been delegated the duties assigned to the DoD Executive Agent for Information Technology Standards.

Gregory E. Saunders
Director, Defense Standardization Program Office

MESSAGE FROM THE DoD EXECUTIVE AGENT FOR IT STANDARDS

By Michael O'Connor
Chief, DISA Interface Standards Division

DoD's IT standards program has two primary goals:

- Improve interoperability, scalability, effectiveness, and efficiency of DoD's IT and national security systems
- Facilitate DoD's transformation to enhance the net-centric capabilities of the warfighter and supporting business operations.

To achieve these goals, the DoD Executive Agent for IT Standards oversees efforts such as the following:

- Identify and assess relevant emerging technologies and related standards
- Manage DoD participation in external IT standards developing organizations (SDOs) and standards setting organizations (SSOs)
- Facilitate feedback and dissemination of IT standards information among stakeholders
- Develop, acquire, adopt, specify, maintain, and manage the life cycle of IT standards for DoD.

The IT standards program management strategy is built around initiatives in three major areas:

- *IT standards governance.* The IT standards governance process selects the best available standards, develops standards portfolios, and adopts them for DoD use. The approved and mandated standards and profiles are retained in the DoD Information Technology Standards Registry (DISR). DISR is hosted on a web-based applica-



Michael O'Connor
Chief, DISA Interface Standards Division

tion tool called DISRonline. DISRonline also hosts other information relating to the IT standards life cycle and the management actions and activities that assist the DoD acquisition and requirements communities with their interoperability efforts. Three articles address our IT standards governance initiatives: Jerry Smith and Walt Okon provide an overview of the governance structure and process, Dave Brown and Jerry Smith discuss how to find the right standards, and Ken Dolson and Doris Bernardini describe the DISR process and DISRonline.

- *Participation in relevant external SDOs/SSOs.* DoD must ensure that its requirements are met with accredited standards that are available from or under development by authoritative non-government sources. When warfighter and business operations have requirements for which there are no available open accredited standards, or that can be met only partially by existing standards, DoD participates in relevant external SDO/SSO activities to ensure the timely consideration of DoD requirements. The SDO/SSO Collaboration Tool is an online capability to facilitate DoD participation in the right external IT standards activities and is described in an article by Robert Kidwell, Joe Brazy, Chris Kreiler, and Nonna Bond. The articles by Jerry Smith and Dennis Devera give us a perspective of our involvement in external global IT standards activities. Finally, Nonna Bond and Chris Kreiler explain “harvesting”—a method for creating an ISO standard from a military specification.

- *Compliance testing and certification.* Validation testing of IT standards and testing of DoD

systems for conformance with IT standards ensure that the implementation of standards across DoD is consistent and in compliance with mandated standards. Certification of systems for interoperability is also essential to ensure that DoD’s requirements are being satisfied by the selected standards and that battlefield interoperability is enabled. The article by Ned Roper, Lylha Cahill, and Steve Cole explains how this important function contributes to achieving interoperability.

The IT standards program management strategy features a proactive management structure, clear yet flexible processes, and a life-cycle approach to the development and promulgation of IT standards, testing and certification, configuration management, sun-setting of IT standards still essential for the interoperability of legacy systems, and retirement of standards that are no longer needed. This strategy applies to DoD components that develop IT standards, use IT standards and profiles, or have an interest in the development of IT standards. Top-level DoD executive participation, oversight, and governance of the IT standards program are provided by the IT Standards Oversight Panel and the Information Technology Steering Committee. Our guiding principle is to separate management of the standards process from the substantive content. An article by Jerry Smith discusses the strategy and principles guiding the IT standards program. In another article, he discusses lessons learned in IT standards development.

A number of laws and regulations mandate the use of technical standards developed by voluntary consensus standards bodies to attain greater reliance on voluntary standards and conformity assessment bodies and to participate in external

SDOs and SSOs. We appoint the official technical experts who represent the warfighter and business operations requirements in appropriate non-government standards development efforts. Our strategy is to increase the availability of open IT standards for DoD use in leveraging net-centric technologies and capabilities and ensuring their widespread visibility. In his article, Jim Hall, Assistant Deputy Under Secretary of

required products increases while making newly developed products more marketable globally. As a result, more conforming products are readily available in the marketplace.

DoD IT standards are prescribed to enable warfighter and DoD business operations to operate in a net-centric environment efficiently and effectively to protect and exchange information.

Our goal is to help program and project managers make well-informed decisions and leverage limited resources to maximum advantage by identifying, developing, prescribing, and implementing the IT standards that best satisfy DoD needs.

Defense for Logistics and Materiel Readiness/ Logistics Plans and Programs, articulates the significance of this important policy regarding the DoD preference for open standards.

By driving the incorporation of requirements—of warfighters, users, consumers, and business operations—into open information and communications technology standards, we encourage industry to develop and build compliant commercial products. As more and more vendors offer such products, prices go down, the number of standardized products goes up, and reliability, robustness, and interchangeability increase. This significantly enhances interoperability. When users and consumers influence the specification of international standards, competition to deliver

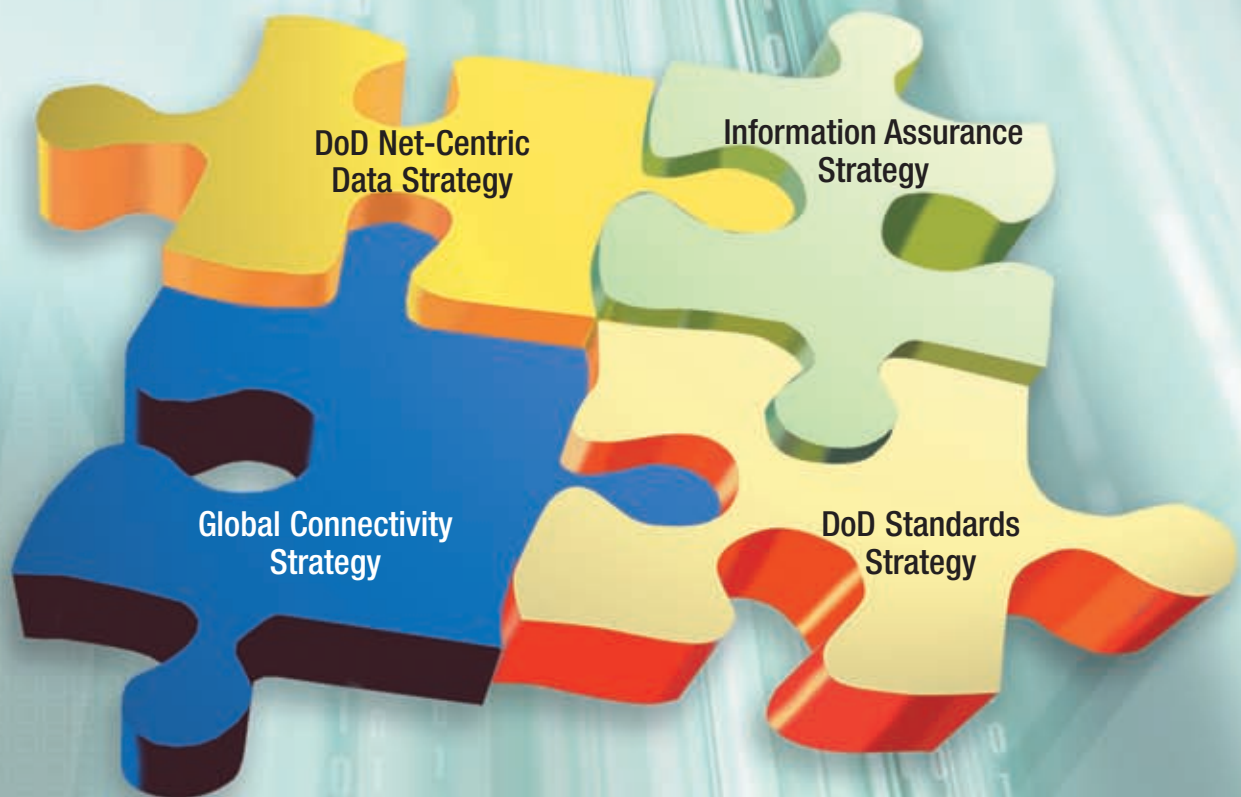
Selection of the “right” standards based on appropriate technology will help us transform to a net-centric environment and facilitate interoperability. Market-supported, open, non-government standards are becoming increasingly important to achieving the scalability and interoperability that are critical to this environment.

We need to determine which technologies, standards, and products best function together to form interoperable and scalable solutions. Our goal is to help program and project managers make well-informed decisions and leverage limited resources to maximum advantage by identifying, developing, prescribing, and implementing the IT standards that best satisfy DoD needs.

“Openness”

An Important Principle for the Stewardship of DoD IT Standards

By Jim Hall



In discussions about IT standards, we often hear the term “open.” The mandated use of open standards by DoD is not only desirable, but is necessary for practical legal and cost reasons:

- If we were to place in our official registry of mandated standards a proprietary specification that belongs to Vendor A or to Consortium B, then DoD would be put in a position of non-competitively “favoring” that entity at the expense of others and accordingly may be subject to potential legal liability.
- If a party in a consortium provides certain intellectual property that is incorporated into one of the consortium’s specifications, and DoD places this particular specification into its official registry of mandated standards, then DoD may be liable for future royalty payments for employing that intellectual property.

These two simple examples demonstrate the importance of ensuring that the standards and specifications adopted by DoD are publicly available and are unencumbered by patents, copyrights, intellectual property rights (IPR), and royalties.

About Open Standards and Specifications

Standards and specifications are considered open—as opposed to proprietary or “closed”—when sponsored and supported by an organization that uses an open, public consensus process to develop and maintain them. This includes control of the document (hard copy or electronic versions) and the absence of IPR issues.

In direct contrast, closed standards and specifications are arbitrarily “controlled,” usually as proprietary. DoD’s main issue with proprietary standards is that they promote vendor lock-in and exacerbate problems with legacy systems. Business enterprises, consumers, and governments alike pay dearly when locked into proprietary solutions.

When applied to the standards creation process, the term “open” means that participation is available to all interested parties who are directly and materially affected. Participation is not conditional upon membership in any organization, nor is it unreasonably restricted on the basis of certain qualifications. All participants have the opportunity for their views and opinions to be heard during the development, approval, adoption, and distribution processes. The development and approval processes must be free from undue influence or dominance by any special or single interest. The development and adoption processes are thought to be open when the normal creation, review, adoption, and publication of technical standards and specifications have the following characteristics:

- The “owning” organization completely and fully discloses the development

process and products. The organization uses a public consensus process to develop, maintain, and manage the configuration of its products.

- IPR issues are absent. A written and publicly available statement delineates the attitude of the organization and its members regarding IPR for patents, disclosure, copyrights, royalties, distribution rights, trademark rights, original contributions, and so on.
- The owner of products published by the organization is clearly and unambiguously identified and is responsible for version control of the products. The owner uses a formal change control process to manage changes to the products and has mechanisms in place to track versions, fixes, and addendums.
- The products and the procedures governing the work of the organization are available (but not necessarily without fee) to any interested party.

In addition to the characteristics of openness, DoD considers the following when selecting open standards for use:

- The standards developing organization (SDO) or standards setting organization (SSO) has established its position within the relevant technical, professional, and marketplace communities as an objective authority.
- The SDO/SSO is accredited or formally recognized as an authoritative body that produces and distributes formal, publicly available standards and specifications.

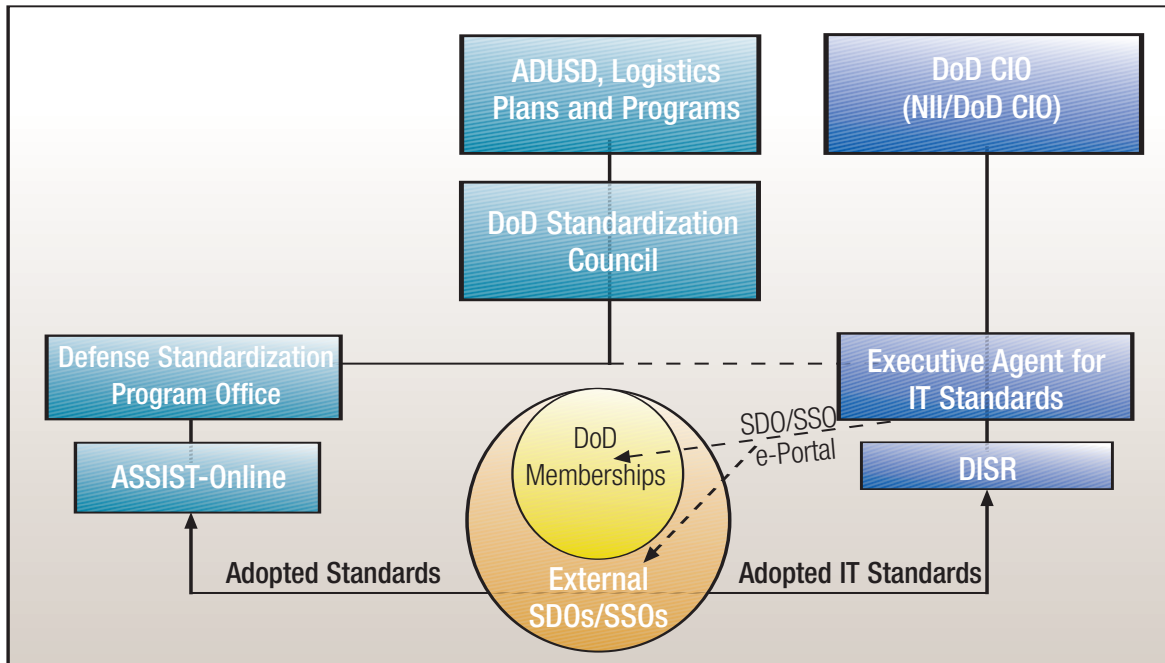
DoD's Open Standard Adoption Strategy

The DoD strategy for adopting open IT standards is to participate in SDOs and SSOs that address emerging information and communications technologies. DoD participants in such organizations ensure that our requirements are considered in deliberations for the standards being developed by the SDO/SSO and that published standards are open and widely available. It is paramount for DoD to be actively involved in relevant SDOs and SSOs so that our requirements for net-centricity are incorporated as part of the published open standard. By incorporating these DoD requirements into open information and communications technology standards, we encourage the private sector to design and build commercial products that comply with the standards.

We recognize that the IT standards-making process will always be outstripped by the pace of technology evolution. DoD participants in external SDO/SSO activities are key links in identifying emerging technologies and standards that will support the DoD net-centric transformation programs, and they must be diligent to provide this important feedback information to priority programs and engineering support activities.

The chief principle is to rely upon the marketplace to build products to the open standards that are essential to DoD’s warfighting and business operations. This principle also applies to non-IT standards that are adopted by the Defense Standardization Program Office (DSPO). Figure 1 shows the relationship of the IT standards and the DSPO standards program.

FIGURE 1. DoD Standards Program Structure



Summary

The National Defense Strategy clearly states how DoD will operate in the future: “we will be net centric. Our job is to deliver the critical enabling capability to conduct network-centric operations.” Open standards are essential building blocks for realizing the DoD Global Information Grid, making the transition to a net-centric environment, and realistically obtaining interoperability. Market-supported open standards will be indispensable for DoD to exchange information seamlessly.

About the Author

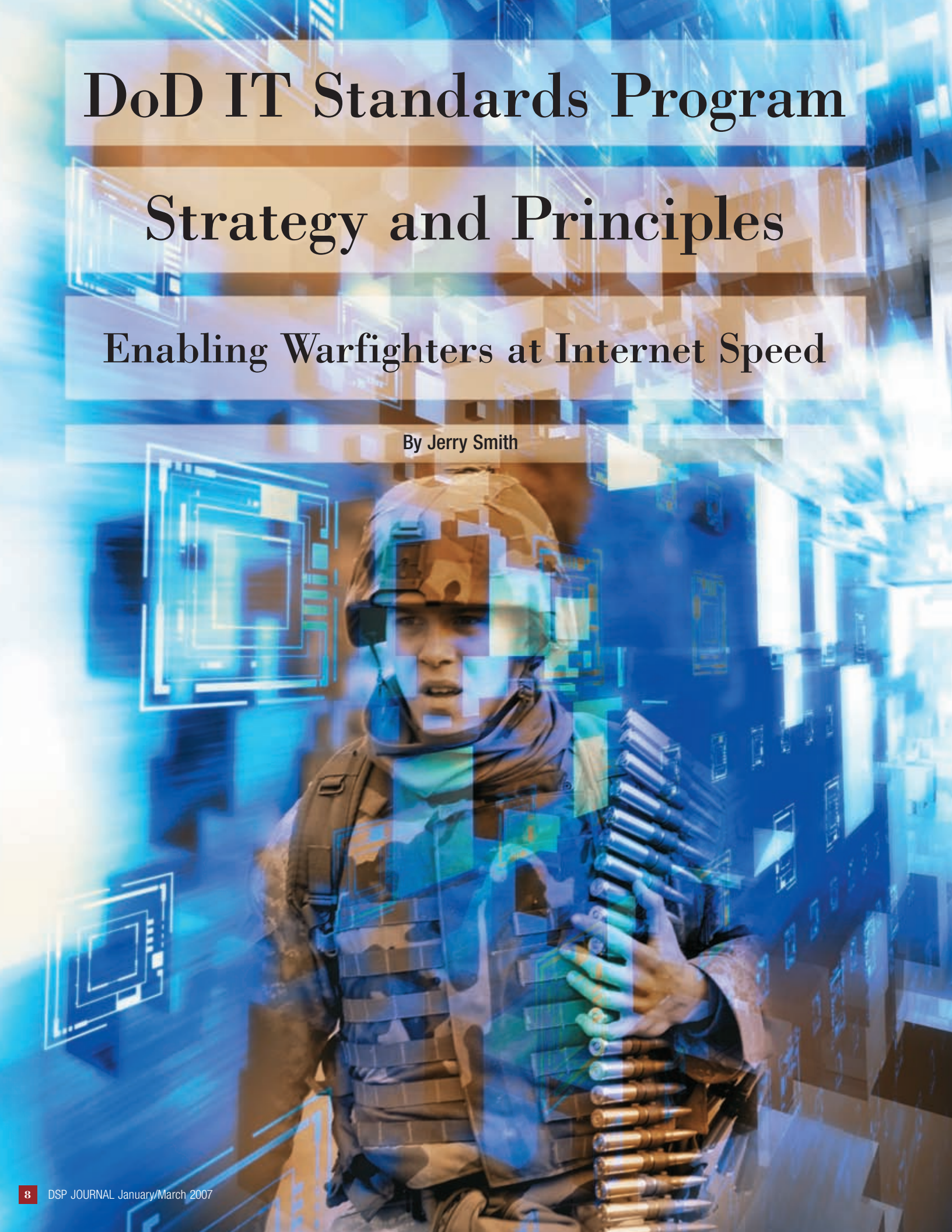
Jim Hall is the DoD Standards Executive and the Assistant Deputy Under Secretary of Defense for Logistics and Materiel Readiness/Logistics Plans and Studies.✱

DoD IT Standards Program

Strategy and Principles

Enabling Warfighters at Internet Speed

By Jerry Smith



The Defense Department's vision is for net-centric operations and warfare:

The National Defense Strategy clearly states how we will operate in the future—we will be net centric. Our job is to deliver the critical enabling capability to conduct network-centric operations. Defense transformation hinges on the recognition that information is our greatest source of power. We can leverage information to allow decision makers at all levels to make better decisions faster and sooner. (John Grimes, DoD Chief Information Officer, March 2006)

The IT standards program is a key element in enabling net-centric transformation. IT standards enable information to be protected by identity-based capabilities that allow users to connect, be identified, and access needed information in a trusted manner—all in a world in which the information is virtual and on demand with global reach.

The Global Information Grid (GIG) is a web-like enterprise and infrastructure in which we can discover information, orchestrate an operational picture based on the situation at hand, have shared situational awareness, and operate securely. Open IT standards will enable Internet technology at speeds capable of bringing people together rapidly and efficiently, help them do their jobs in new ways never before anticipated, and help them accomplish their missions as never before envisioned.

DoD Executive Agent for IT Standards

The Director, Defense Information Systems Agency (DISA), is designated as the DoD Executive Agent (EA) for IT Standards. The duties assigned to the EA have been delegated to the Interface Standards Division in the DISA GIG Enterprise Services Engineering Directorate of the Systems Engineering, Architecture and Integration Center. The EA duties are as follows:

- Centrally manage the IT standards program in accordance with DoD Directive 5101.7, “DoD Executive Agent for Information Technology Standards,” May 2004.
- Develop, with DoD components, a standards management strategy and program plan that implements the requirements of various public laws and statutes. Examples are Section 2223, Title 10 of the United States Code; DoD Directive 4630.5, January 11, 2002; and DoD Instruction 4630.8, June 30, 2004.
- Manage and oversee the identification, adoption, specification, and life-cycle configuration management of IT standards that apply throughout DoD. These standards are to help achieve interoperable IT and national security systems (NSS) and to contribute to decision superiority in support of net-centric operations.

Strategy

The EA has identified two goals for the IT standards program:

- Improve interoperability, scalability, effectiveness, and efficiency of DoD's IT and NSS
- Facilitate the net-centric capabilities of the warfighter and DoD business operations.

The strategy is to ensure that DoD requirements are met within accredited non-government standards—open, market supported, and from authoritative sources—that are available or under development. This is consistent with public law, judicial precedent, and extant policy of the federal government and DoD.

The national standards strategy developed by the American National Standards Institute (ANSI) encourages the reliance on a voluntary, consensus-based process to develop market-endorsed open standards that support the global competitiveness of the United States. DoD supports ANSI's strategy and encourages the establishment of partnerships and collaboration with relevant external standards developing organizations (SDOs) and standards setting organizations (SSOs) of interest specifically to meet DoD needs.

DoD's strategy for the IT standards program is to use accredited standards from authoritative sources in accordance with DoD policy and preferences to satisfy requirements with open, consensus-based public- and private-sector standards. Our experience shows that this approach reduces costs and enhances vendor-supported product availability. Also, the responsible SDO or SSO, because of its established position within the relevant technical, professional, and marketplace communities, is an objective authority, which implies that the standards developed by the organization are widely accepted and have been successfully implemented in the marketplace. The requirement for open IT standards is not simply a desired characteristic; it is

based on practical legal and cost considerations. Standards must be publicly available and free from patents, copyrights, intellectual property rights, constraints, and royalties.

By advocating for the incorporation of DoD requirements into open commercial standards, DoD encourages industry to design and build compliant commercial off-the-shelf (COTS) products that will enable DoD to operate effectively in a net-centric environment.

RATIONALE

DoD needs to use commercially available open standards-based products that work together seamlessly and can be integrated into existing business processes and warfighter systems. The solutions supported by the selected open standards must be scalable and interoperable.

The right standards solve user problems as manifested in well-designed and efficient business processes, reflect available and relevant technology, and have market support in that vendors have built conforming products that are available in the marketplace.

By driving the incorporation of user, consumer, and business operations requirements into open information and communications technology standards, DoD encourages industry to develop and build compliant commercial products that are available as conforming COTS products. As more and more vendors offer compliant COTS products, prices go down, the number of standardized products goes up, and reliability, robustness, and interchangeability increase. This significantly enhances interoperability. When users and consumers influence the specification of international standards, competition to deliver required products increases while making newly developed products more marketable globally. As a result, more conforming products are readily available in the marketplace.

MANAGEMENT APPROACH

The IT standards program management strategy is built around three major areas: IT standards governance, participation in relevant external SDOs and SSOs, and standards testing to ensure compliance. In the case of IT standards that are not supported commercially, that is, standards (such as some satellite standards) that have only military application, DoD follows the MilStd development processes prescribed in DoD Directive 4120.24, “Defense Standardization Program (DSP).”

The IT standards governance process selects best available standards, develops standards portfolios, and adopts them for DoD use. The approved/mandated standards and profiles are retained in the DoD IT Standards Registry (DISR), which is hosted on a web-based application tool called DISRonline. DISRonline also hosts other information relating to IT standards life-cycle and management actions that assist the DoD acquisition and requirements communities with their interoperability efforts.

When warfighter and business operations have requirements that cannot be met with available open

accredited standards or that can be met only partially, DoD participates in relevant external SDO/SSO activities to ensure that its requirements can be addressed in a reasonable time frame.

DoD IT standards governance and SDO/SSO participation are linked. Emerging technology and standards trends, coupled with DoD IT interoperability needs, can be identified through work in the SDO/SSO and brought forward to the IT standards governance process. By promoting the development and use of open market-supported, non-government standards whenever possible, the IT standards program will support transformation to a net-centric environment, reduce costs, and achieve the interoperability necessary for net-centric warfighting functions and DoD business operations. When open accredited standards cannot satisfy DoD systems’ requirements, the EA actively participates as a key player at the military, national, and international levels to provide management and technical expertise in developing the needed standards.

Validation testing of IT standards and testing of DoD systems for conformance ensures that the im-

IT Standards Development Principles

Participation is fully open to interested parties who are directly and materially affected.

Participation is not conditional upon membership in any organization or unreasonably restricted on the basis of certain qualifications.

There is opportunity for the views and opinions of all participants to be inputs to the development, approval, adoption, and distribution processes.

The development/approval process is free from undue influence or dominance by any special or single interest.

The products, and the procedures governing the work, of the organization are available (but not necessarily without fee) to any interested party.

plementation of standards across DoD is in compliance and consistent with mandated standards. Certification of systems' interoperability is also essential to ensure that DoD's requirements are being satisfied by the standard.

The IT standards program strategy features clear, yet flexible, processes and a life-cycle approach to the development and promulgation of IT standards, testing and certification, configuration management, sun-setting of IT standards still essential for legacy systems interoperability, and retirement of standards that are no longer needed. This strategy applies to DoD components that develop IT standards, use IT standards and profiles, or have an interest in the development of IT standards.

Principles

An important principle of the IT standards program is the separation of the management of standardization activities from the technical work. IT standards activities are managed within a life-cycle portfolio; decisions are based on mission goals, architecture,

risk, performance, and expected return on investment. Technical work is based on IT interoperability needs, DoD requirements, and technology evolution or revolution. DoD must also consider priorities for transformation to a net-centric environment for war-fighter and business operations. The management principle is that the EA owns the IT standards management process, and the sponsors and stakeholders across the enterprise own the substantive content.

GOVERNMENT ROLE

In the United States, there is a strong orientation toward relying on private enterprise to lead voluntary standards activities. Standards are validated by marketplace acceptance when vendors produce COTS products based on open standards. For DoD, this is usually the most efficient and cost-effective approach to IT standardization. However, left to its own devices, the U.S. voluntary standards system does not always reliably produce all of the standards that DoD needs. The IT standards program will work with the private sector to help ensure that DoD requirements are incorporated into the needed open standards.

IT Standards Program Management Principles

Manage IT standards as a portfolio. A portfolio is a group of standards and activities related to a specific technology area.

Rely on open private-sector-produced IT standards availability.

Replicate good, proven business practices.

Keep pace with technology evolution.

Employ a life-cycle approach to standards management.

Make standards visible and available.

Understand that the Executive Agent owns the standards management process, while the sponsor/stakeholder owns the substantive content of the standard.

Leverage technology and tools for maintaining a "paperless" environment.

Involve stakeholders.

Monitor the timing of building and mandating standards in relation to technology. Timing is critical. Setting standards too early could stifle innovation and creativity; setting them too late could engender social and economic costs.

When creating standards, specify performance and interface requirements, not the process for building the end product.

STRATEGIC STANDARDIZATION

Strategic standardization is important to the U.S. economy. It is an effective management tool for businesses to gain a leading edge on competition or protect a competitive position. DoD's stake in strategic IT standardization is rooted in the fact that a strong defense is based on a strong economy, and a strong economy depends on maintaining global competitiveness. IT standards are a key enabler to achieving and maintaining global competitiveness. U.S. global leadership of IT standards and leading-edge technology is a critical factor to the future health and vitality of our economy. It is in DoD's long-term best interest that the U.S. IT industry is healthy and robust and maintains its current global leadership position. DoD representatives to SDOs/SSOs at national and international levels must keep this in mind when preparing DoD positions for input into these organizations.

DOD INVOLVEMENT IN EXTERNAL STANDARDS ACTIVITIES

Externally developed, non-government standards are becoming increasingly important to achieving scalability and interoperability throughout DoD. By promoting the development and use of market-supported, open non-government standards whenever possible, the IT standards program will support transformation to a net-centric environment, reduce costs, and achieve the interoperability necessary for net-centric warfighting functions and DoD business operations. When standards sponsored by the private sector cannot satisfy DoD systems requirements, the EA actively participates as a key player at the military, national, and international levels to provide management and technical expertise in developing the required IT standards deliverables. By influencing the specification of international standards, competition to deliver required products increases while making newly developed U.S. products more marketable globally.

Public law and federal government policy mandate DoD participation in external standards forums to lead and influence open private-sector-based IT standards activities. To that end, a set of objective criteria have been established for evaluating and ranking the various SDOs/SSOs. These criteria will also help determine which standardization paths will provide the best mechanism for the development, adoption, and publication of the IT standards needed by DoD. DoD representatives must work with SDOs/SSOs to incorporate warfighter and business operations requirements into standards and drive the availability of open, standards-based products.

Summary

DoD's overall strategy is to rely on the private sector to build the open standards that are needed. DoD participates as equal partners in as many SDOs and SSOs as possible. The reasons for DoD's participation are twofold: provide input on DoD requirements into the standards-building process, and bring back to DoD stakeholders information about technology standards trends and activities.

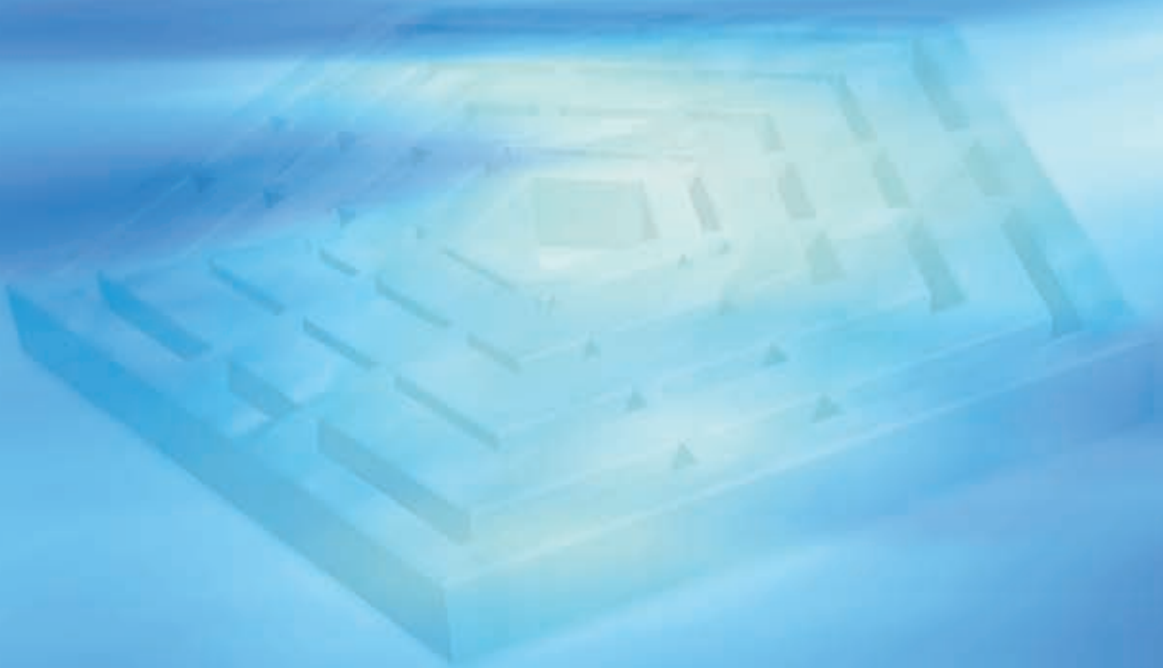
The IT standards program management approach is proactive, with flexible open processes to ensure that DoD can capitalize on getting its requirements into commercially available standards developed by recognized and authoritative external SDOs and SSOs. The strategy recognizes that the right IT standards are key enablers to fast and accurate information awareness and exchange across the enterprise.

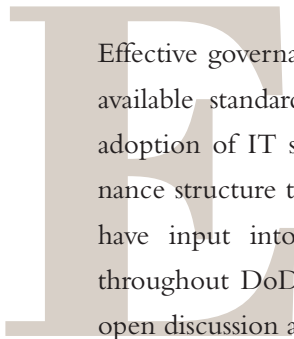
About the Author

Jerry Smith is a computer scientist in the Interoperability Standards Division of the Defense Information Systems Agency, DoD's Executive Agent for centralized life-cycle management of IT standards. Mr. Smith is coordinating DoD's participation in global private-sector IT standards activities. ✨

Governance of IT Standards

By Walt Okon and Jerry Smith





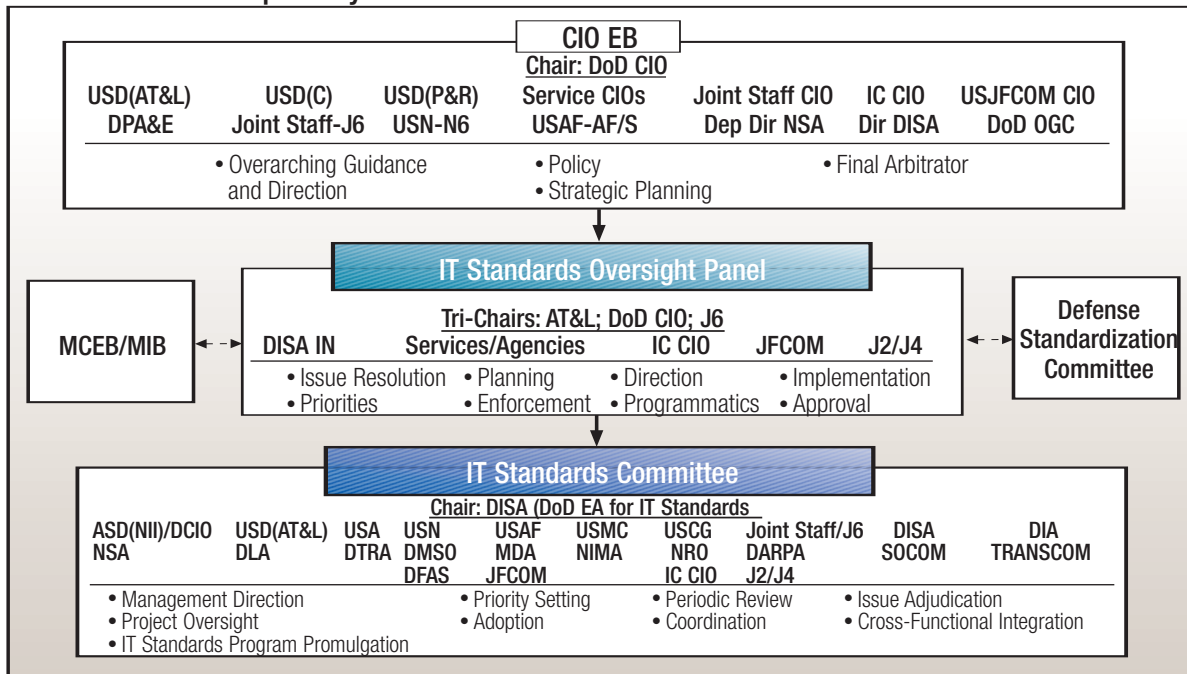
Effective governance of IT standards is crucial to ensure the selection of the best available standards, development and maintenance of standards portfolios, and adoption of IT standards for DoD use. Therefore, DoD has established a governance structure that provides an opportunity for a wide-range of DoD entities to have input into the standards selection process. It encourages participation throughout DoD and maintains a flexible, responsive environment to encourage open discussion and exchange of ideas to meet DoD requirements.

The key entities involved in governance of IT standards are the DoD Executive Agent (EA) for IT Standards, the Chief Information Officer (CIO) Executive Board, the IT Standards Oversight Panel (ISOP), and the IT Standards Committee (ITSC), including its subcommittees and technical working groups (TWGs). Below, we describe some of the governance activities for which these entities are responsible. Figure 1 shows the relationship of the key entities in IT standards governance.

DoD Executive Agent for IT Standards

The Deputy Secretary of Defense has designated the Director, Defense Information Systems Agency (DISA), as the EA for IT Standards. The duties assigned to the EA have been delegated to the Interface Standards Division in the DISA Global Information Grid (GIG) Enterprise Services Engineering Directorate of the Systems Engineering, Architecture and Integration Center. The chief responsibility of the EA is to centrally manage the IT standards program for DoD, ensuring the selection of the best available standards, development of standards portfolios, and adoption of the standards for DoD use.

FIGURE 1. Relationship of Key IT Governance Entities



Entities Involved in Governance of IT Standards

Chief Information Officer Executive Board

DoD Chief Information Officer (Chair)
Under Secretary of Defense (Acquisition, Technology and Logistics)
Under Secretary of Defense (Comptroller)
Under Secretary of Defense (Personnel and Readiness)
Air Force (AF/S)
Air Force Chief Information Officer
Army Chief Information Officer
Deputy Director, National Security Agency
Director, Defense Information Systems Agency
Director, Program Analysis and Evaluation
DoD Office of General Counsel
Intelligence Community Chief Information Officer
Joint Staff Chief Information Officer
Joint Staff (J6)
Marine Corps Chief Information Officer
Navy Chief Information Officer
Navy (N6)
U.S. Joint Forces Command Chief Information Officer

IT Standards Oversight Panel

DoD Chief Information Officer (Tri-chair)
Joint Staff (J6) (Tri-chair)
Under Secretary of Defense (Acquisition, Technology and Logistics) (Tri-chair)
Defense Information Systems Agency (IN)
Intelligence Community Chief Information Officer
Joint Staff (J2/J4)
Services and Agencies
U.S. Joint Forces Command

IT Standards Committee

Defense Information Systems Agency/DoD Executive Agent for IT Standards (Chair)
Assistant Secretary of Defense (Networks and Information Integration, Deputy Chief Information Officer)
Under Secretary of Defense (Acquisition, Technology and Logistics)
Air Force
Army
Coast Guard
Defense Advanced Research Projects Agency
Defense Finance and Accounting Service
Defense Information Systems Agency
Defense Intelligence Agency
Defense Logistics Agency
Defense Modeling and Simulation Office
Defense Threat Reduction Agency
Intelligence Community Chief Information Officer
Joint Staff (J2/J4)
Joint Staff (J6)
Marine Corps
Missile Defense Agency
National Imagery and Mapping Agency
National Reconnaissance Office
National Security Agency
Navy
U.S. Joint Forces Command
U.S. Special Operations Command
U.S. Transportation Command

DoD Directive (DoDD) 5101.7, “DoD Executive Agent for Information Technology Standards,” encompasses IT standardization in all Lead Standardization Activities (LSAs). DoDD 4120.24, “Defense Standardization Program (DSP),” and DoD 4120.24-M, “Defense Standardization Program Policies and Procedures,” contain complementary direction:

- DISA is designated as the LSA for data communications protocol standards, information standards and technology, information processing standards for computers, and telecommunications systems standards within the Defense Standardization Program.
- The National Geospatial Agency is designated as the LSA for geospatial intelligence standards, including the Imagery Standards Management Committee and Geospatial Standards Management Committee.
- The Defense Modeling and Simulation Office is designated as the LSA for modeling and simulation standards.

Figure 2 depicts the governance structure.

FIGURE 2. Governance Structure

GIG Governance											
NET OPS	System Engineering	Business Subcommittee				Warfighting Subcommittee		National Intelligence Subcommittee			
		Governance				Governance		Governance			
		Installations & Environment Domain	Human Resources Management Domain	Acquisition Domain	Strategic Planning & Budgeting Domain	Logistics Domain	Accounting & Finance Domain	JS/OSD Working Portfolio Definitions & Governance		In work	
		Communications Domain (IPv6, Information Transfer, Messaging, Radio, SATCOM, Transformational Communications)		Computing Infrastructure Domain (Application, Discovery, Mediation, Storage, and User Assistant)		CORE Enterprise Services Domain (Collaboration, Enterprise Service Management)				Information Assurance/Security Domain (IA/Security, including Biometrics)	
		Governance						Governance		National Intelligence Enterprise Information Environment Subcommittee	
		Enterprise Information Environment Subcommittee									

CIO Executive Board and IT Standards Oversight Panel

The CIO Executive Board maintains the overall oversight of the IT standards process. The board provides overarching guidance and direction, policy, and strategic planning and is the final arbiter of issue disputes.

The ISOP assists with planning, sets priorities for the ITSC, and provides direction and resolution for issues originating within the ISOP, and approves all standards included in the DoD IT Standards Registry (DISR).

IT Standards Committee

The ITSC provides the main technical coordination, cross-functional integration, and collaboration among the ITSC subcommittees. The ITSC also promulgates standard operating procedures and adjudicates issues arising from the ITSC subcommittees. Currently, the ITSC has four subcommittees: business, warfighting, enterprise information environment, and national intelligence.

The ITSC is the EA's DoD IT standards coordination body consisting of representatives of the services, agencies, and combatant commands. These representatives help with assigning subject matter experts (SMEs) to TWGs charged with vetting IT standards and standards profiles to adopt and mandate for DoD use.

During TWG deliberations, each SME represents his or her sponsor's position while negotiating to reach consensus. Consensus is defined as a general agreement characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests, and by a process that involves seeking to account for the views of all parties concerned and to reconcile any conflicting arguments. Consensus does not imply unanimity.

ITSC Subcommittees

The ITSC subcommittees are established to pursue standards identification, development, adoption, and review, as well as configuration management activities. The subcommittee chairs, who are appointed by the EA, ensure that the ITSC and ISOP are notified of content changes to the portfolio. Content changes also affect the DISR.

Technical Working Groups

The TWGs, which are subordinate to the ITSC subcommittees, consist of SMEs from standards sponsors and stakeholders. The TWG chairs are responsible for submitting findings and recommendations to their subcommittee chairs.

The TWGs do the technical work on IT standards for their respective subcommittees. The SMEs discuss and determine the requirement for a standard, hold discussions, and recommend adoption—based on such criteria as public availability, the standard's implementation in vendor products, and the standard's maturity—for implementation by DoD program managers. TWGs promote interoperability

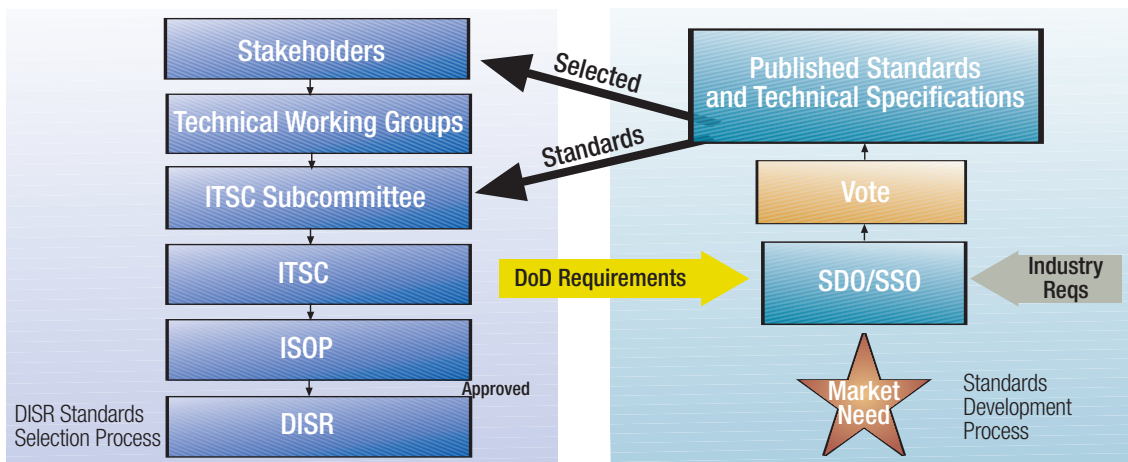
through implementation guidance on standards in their area of assignment and manage changes to standards portfolios.

TWGs coordinate and integrate all actions assigned within their function or portfolio activity area, including appropriate support to DoD standardization executives and LSAs in developing, adopting, specifying, and testing IT standards.

When standards are readily available to meet its requirements, DoD will select the best and most cost-effective standards. When there are gaps between the DoD requirements and standards, or no standard yet exists to meet DoD's requirements, DoD works with public and private-sector standards developing and standards setting organizations (SDOs/SSOs) to ensure that DoD requirements are considered in the IT standards development process. Figure 3 depicts the general working relationship of TWGs and SDOs/SSOs. This process shows the life cycle of a standard from idea to adoption and recording of the standard in the DISR.

Published standards developed within the SDO/SSO environment are selected and adopted by the TWGs, approved by the ITSC subcommittee chairs, and forwarded to the ITSC for consideration. The ITSC will forward its recommendations to the ISOP for approval and authority to promulgate. Upon adoption, standards are registered and stored on the DISRonline. The ITSC subcommittee is responsible for moving a standard through its life cycle.

FIGURE 3. Relationship between Technical Working Groups and SDOs/SSOs



About the Authors

Walt Okon is a senior staff member of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Office. He has oversight responsibilities for the DoD Executive Agent for IT Standardization.

Jerry Smith is a computer scientist in the Interoperability Standards Division of the Defense Information Systems Agency and coordinates DoD's participation in global private-sector IT standards activities. ✨

Finding the Right Standards

By Dave Brown and Jerry Smith

ISO 10303



Anyone who has tried it knows: finding the right IT standards is not easy. One issue is that navigating today’s complex and volatile standards environment is time-consuming and expensive. Another is that there is no recognized, readily accessible, and unbiased source of information that answers scalability and interoperability questions reliably and objectively.

Value Proposition

Participation in standards development can be very expensive, in view of the investments in time (labor) and travel costs. However, on the benefit side of the equation, finding the right standards is of strategic importance for building better, cost-effective weapons systems while achieving interoperability with our coalition partners. An early investment in developing open standards can reap huge savings in weapon system acquisition costs. For example, the Department of Commerce estimates that ISO 10303, “Standard for the Exchange of Product Model Data”—a private-sector standard for which DoD played a major development role—could save \$928 million per year by reducing interoperability problems in the automotive, aerospace, and shipbuilding industries.¹

A goal of the IT standards program is to determine which standards and products best function together to form interoperable and scalable solutions. Unfortunately, thousands of candidate standards and myriad global groups and activities address—and often perform duplicated work on—the same issues. There are simply too many standards developing organizations and standards setting organizations (SDOs/SSOs) to track them all, let alone influence the incorporation of DoD requirements into the standards they develop.

Thus, finding the right standard is a difficult and risky task.

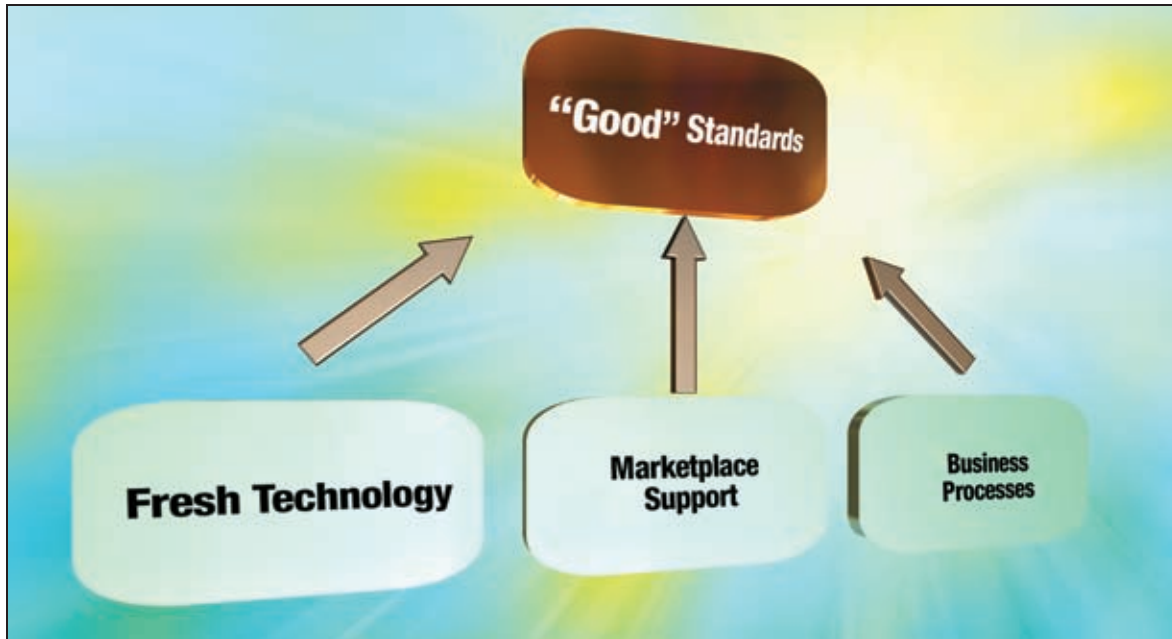
What Are “Good” Standards?

The key drivers of “good” IT standards are fresh technology, marketplace support, and business processes, as shown in Figure 1.

Good standards solve user problems as manifested in well-designed and efficient business processes, reflect available and relevant technology, and very importantly have market support, in that vendors have built conforming products that are available in the marketplace.

DoD must use commercially available open standards-based products that seamlessly work together and can be integrated into existing business processes and warfighter systems. The solutions supported by the selected open standards must be scalable and interoperable.

FIGURE 1. Enablers of “Good” Standards



The goal of the DoD IT standards program is to help program and project managers make well-informed decisions by identifying, developing, prescribing, and implementing the IT standards that best satisfy DoD needs to protect and exchange information. The strategy is to use accredited standards from authoritative sources in accordance with DoD policy and preferences.

A net-centric environment uses a web-based infrastructure to allow people throughout the enterprise to access and share information for total situational awareness and superior decision making. Market-supported, open, non-government standards are becoming increasingly important to achieving the scalability and interoperability that are critical to this environment.

DoD Requirements

A number of laws and regulations mandate the use of technical standards developed by voluntary consensus standards bodies, to attain greater reliance on voluntary standards and conformity assessment bodies.² The U.S. National Standards Strategy encourages reliance on a voluntary, consensus-based process to develop market-endorsed open standards that support the global competitiveness of the United States.

DoD has established a long-standing hierarchy of preference for selecting standards on the basis of their source. Table 1 shows that hierarchy.

TABLE 1. Standards Preference Hierarchy

Priority	Standards source hierarchy	Examples
1	International	International Electrotechnical Commission International Organization for Standardization International Telecommunication Union
2	National	American National Standards Institute
3	Professional society; technology consortia; industry association	Government Electronics and Information Technology Association Institute of Electrical and Electronics Engineers Internet Engineering Task Force Organization for the Advancement of Structured Information Standards World Wide Web Consortium
4	Government	Federal Information Processing Standards
5	Military	Military standards Standardization agreements

Strategy

An effective IT standards management program helps make well-informed decisions and leverage limited resources to maximum advantage by identifying, developing, and implementing IT standards that best satisfy DoD needs. This is accomplished by identifying and participating actively in selected external SDOs/SSOs that can contribute directly to DoD’s transformation to a net-centric environment. It also ensures representation of DoD needs in these external organizations. By advocating incorporation of its requirements into open, non-government, “commercial” standards, DoD encourages industry to develop and build compliant commercial products that will enable DoD to effectively operate in a net-centric environment.

The strategy of the Executive Agent for IT Standards is to increase the availability of open IT standards for DoD use in leveraging net-centric technologies and capabilities, to ensure their widespread visibility, and to identify the ones that are most closely aligned with our requirements and priorities. We have developed some selection criteria, outlined in Table 2, to provide an objective framework for identifying the best candidates to include in the DoD IT Standards Registry (DISR).

TABLE 2. Standards Selection Criteria

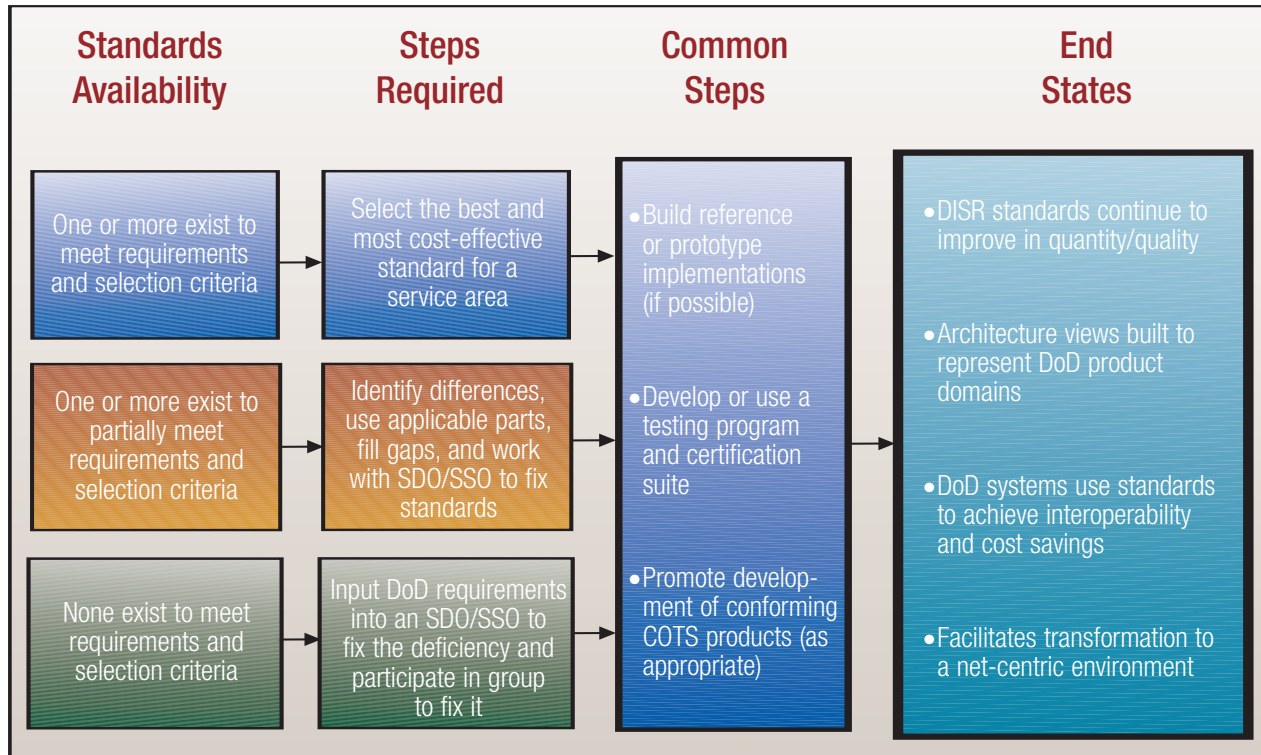
Criterion	Description
Source of the standard	Recognized authority
	Cooperative stance
	Feedback (receptive to user needs, concerns, and appeals)
	Process (development process documented and widely available)
	Consensus (development/approval process free of undue influence or dominance by any special or single interest)
Openness	Ownership (organization policies regarding document ownership, control, and intellectual property rights)
	User participation
	Vendor participation
Technology relevance	Applicability to current DoD objectives (technically feasible/commercially viable; “state-of-art” vs. “state-of-practice”)
Maturity	Planning horizon (length of time standard has existed or length of time standard should be useful)
	Stability
	Revision content and schedule
Marketplace support	Acceptance
	Commercial viability
Usefulness/utility	Well-defined quality attributes
	Services and application interoperability
Risk	Issues regarding performance, maturity, and stability

What Are the “Right” Standards?

DoD prefers to satisfy its requirements with open, consensus-based public- and private-sector standards that are currently available or under development. Being available from a reputable and authoritative source means that the responsible SDO/SSO must have an established position as an objective authority in its sphere of activity within the relevant technical, professional, and marketplace communities. This also implies that the standards the organization develops are widely accepted and have been successfully implemented in the marketplace. The requirement that IT standards be open is not simply a desired characteristic but based on practical legal and cost considerations. Standards must be publicly available, royalty free, and free from patents, copyrights, and intellectual property rights constraints.

Figure 2 illustrates the process for adopting open standards for DoD. The priority is support for net-centric IT standards.

FIGURE 2. Process for Adopting Open Standards



Summary

DoD prescribes IT standards to enable both the warfighter and DoD business operations to protect and exchange information efficiently and effectively. Selecting the correct IT standards based on appropriate technology will help DoD facilitate interoperability and transform to a net-centric environment.

¹National Institute of Standards and Technology, *Economic Impact Assessment of the International Standard for the Exchange of Product Model Data (STEP) in Transportation Equipment Industries*, NIST Planning Report 02-5, 2002, p. ES-2.

²Examples are United States Code, Title 10, Section 2223; National Technology Transfer and Advancement Act; and “Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities” published as Office of Management and Budget Circular A-119, revised, February 1998.

About the Authors

Dave Brown manages the Standards Engineering Branch within the Defense Information Systems Agency (DISA) Systems Engineering Center. He has been principally involved in the development and promulgation of DoD policy and processes that support the interoperability and supportability of information technology and national security systems. He has served DISA, the DoD Chief Information Officer, and the U.S. Navy in standards management aspects ranging from governance to assessment and compliance.

Jerry Smith is a computer scientist in DISA’s Interoperability Standards Division and coordinates DoD’s participation in global private-sector IT standards activities. ✨

A Behind-the-Scenes Look at Managing DoD/Joint Interoperability

By Ned Roper, Lylha Cahill, and Steve Cole

JCPATE BETA

Navigation: JCPATE Home | Account Management | Register | Submission | Staffing | Assessment | Search | Reports

Welcome Van Functional Analyst | Logout

My Account

Username: **van_fa**
Password Expires in: 63 day(s)

My Queues

My Assessments: 2
My Submissions: 123
Pending Submissions: 128
Available for Staffing: 123

Quick Links

- Submit a Document
- Find a Document
- Find a User
- Edit My Profile
- My Account History
- Register New Program
- Register New System

Most Recent Submissions

- Nov 13, 2006 1:58:46 PM
THEATER MEDICAL INFORMATION PROGRAM
- Nov 13, 2006 9:37:27 AM
26. PROCESSING TOOL
- Nov 10, 2006 6:32:26 PM
SURFACE ELECTRONIC WARFARE IMPROVEMENT PROGRAM
- Nov 10, 2006 5:35:02 PM
GLOBAL COMBAT SUPPORT SYSTEM (GESS)
COMBATANT COMMA

Most Recently Completed Assessments

JCPAT-E Account Status Distribution

Factoid

Status	Count
Active	113
Disabled	8
Interim	20
Denied	1
Pending	54

Event Calendar

Dec 2006

S	M	T	W	T	F	S
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Legend: ● - Comments Due, ● - Draft Due, ● - Final Due

Have you ever picked up your TV remote and pushed button after button, only to realize you had the wrong remote? The remote that operates the ceiling fan is not interoperable with your TV. Similarly, how about the set of speakers you just purchased that don't work with your new 42-inch plasma screen TV—frustrating, isn't it? You could have avoided or minimized such problems if your equipment choices had been governed by a process to review and enforce interoperability beforehand.

Likewise, every management process in the pursuit of DoD/joint interoperability needs an enforcement capability that assists both overseer and implementer. The Interface Standards Division of the Defense Information Systems Agency (DISA) is one of several technical offices within the Office of the Secretary of Defense whose major goal is to manage the process leading to battlefield and business interoperability.

Within the Interface Standards Division is a subordinate branch, Net-centricity, Requirements, Analysis and Assessments Branch (GE333), whose major role is the behind-the-scenes facilitator of the Joint IT and national security systems (NSS) Interoperability Assessment, Test and Evaluation Program and the developer and manager of specialized applications used by key players in the DoD IT community: Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, or OASD(NII)/DoD CIO; the Joint Staff Directorate for Command, Control, Communications, and Computer Systems (J6); and DISA. This community, as well as specialized offices in other DoD components, works closely with GE333 to minimize interoperability issues across DoD. GE333 serves as the front-end manager of network-centric reviews, assessments, and analysis geared toward ensuring that DoD programs and systems are interoperable and supportable before they're developed and fielded across DoD.

To facilitate support—as mandated in DoD, Joint Staff, and DISA policies—GE333 provides the IT community with help via the Joint IT and NSS Interoperability Assessment, Test and Evaluation Program. To that end GE333 has operated autonomously as the developer and manager of the original implementation of the Joint C4I Program Assessment Tool (JCPAT) software application and all of its follow-on enhancements. This tool focuses on interoperability- and supportability-based net-centric reviews, assessments, and analysis. JCPAT was the first of its kind to capitalize on the World Wide Web to efficiently facilitate assigned responsibilities and simultaneously support the formal collaboration needs for staffing, assessment, review, and comment between the IT/NSS community and other DoD components via NIPRNet (Unclassified but Sensitive Internet Protocol Router Network) and SIPRNet (Secret Internet Protocol Router Network).

The inception of joint net-centric capabilities, accompanied by the need for timely pretest analysis of net-centric interoperability and supportability, required an upgraded JCPAT application in FY05–FY06. The JCPAT-Empowered (JCPAT-E), as the new application is known, extends the original capability, incorporates DoD-wide usage of the DoD IT Standards Registry, and facilitates program manager enforcement of IT standards development (TV-1 of the DoD Architecture Framework).¹ Its functions have expanded greatly beyond its predecessor's basic beginnings:

- JCPAT-E functions as the formal interoperability and supportability staffing, comment collection, and resolution mechanism for all Joint Capabilities Integration and Development System (JCIDS) documents and all Information Support Plan (ISP) documents as OASD(NII)/DoD CIO directs. This version is the front-end triggering mechanism and support process for the Joint Staff-J6's Joint IT and NSS Interoperability and Supportability assessment, analysis (planned), test, evaluation, and eventual interoperability/supportability certification requirements mandated by the JCIDS and OASD(NII) ISP processes.

JCPAT capitalizes on the World Wide Web to facilitate assigned responsibilities and simultaneously support the formal collaboration needs for staffing, assessment, review, and comment between the IT/NSS community and other DoD components.

- The new application also provides DISA with the needed coordination and collaboration platform to ensure internal ISP verification of policy and procedural matters prior to a document's formal JCIDS or OASD(NII) submission. Through the JCPAT-E, DoD program managers can always view, address, collaborate on, and consider DoD-wide recommendations on interoperability, supportability, and information assurance, and receive pre-evaluation of Net Ready Key Performance Parameter requirements and products before deciding to release a document for submission via GE333.


JCPAT-E and the various subprocesses it supports involve centralized management; assessor/program manager collaboration; and availability and retention of pertinent interoperability and supportability assessment and analysis information for DoD, Joint Staff-J6, and OASD(NII)/DoD CIO. Its critical linkage to the JCIDS processes and procedures of the Joint Staff Force Structure, Resources and Assessment Directorate (J8) ensures that all GE333, Joint Staff-J6, and OASD(NII)/DoD CIO assessors are supported by the tenets of handling information only once.

JCPAT-E upgrades planned over the next 3 years will involve the consumption and production of web services, real-time collaboration, content discovery, and single-person assessment management. To help users access program- or system-specific information in other related DoD support applications, JCPAT-E will capitalize on binary-XML web service techniques for smoothing out the process and flow between certain applications. Specifically, JCPAT-E's content discovery functions will produce an awareness (accountability) of JCIDS artifacts, a top-down system evaluation using data mining techniques (dashboards), stronger application management with deeper operations metrics, and smarter searches of systems metadata and binary file attachments.

¹The TV-1 is one of the 15 architecture products required by the mandatory Net Ready Key Performance Parameter (NR-KPP) product table, outlined in Chairman of the Joint Chiefs of Staff Instruction 6212.01D.

About the Authors

Ned Roper is chief of DISA's Netcentric Interoperability Assessments Branch and the facilitator of DoD's Joint IT and NSS Interoperability Assessment, Test and Evaluation Program. He has more than 30 years of experience in communications enhancement for the U.S. Army and Joint communities.

Lylha Cahill is the project manager for JCPAT-E and the Netcentric Interoperability Assessments Program. Steve Cole is the assistant project manager for JCPAT-E. Both Ms. Cahill and Mr. Cole have extensive experience with DoD joint programs. 

Collaborating with External Organizations to Develop and Set IT Standards

By Jerry Smith



The U.S. National Standards Strategy, developed by the American National Standards Institute, encourages reliance on a voluntary, consensus-based process to develop market-endorsed open standards that support the global competitiveness of the United States. DoD supports that strategy, and it encourages collaboration and partnering with relevant external standards developing and standards setting organizations (SDOs/SSOs) that can help meet DoD needs.

Current Environment

DoD prescribes IT standards to enable both warfighters and business operations to protect and exchange information. Selecting the correct IT standards, based on appropriate technology, will help DoD to facilitate interoperability and transform to what is known as a “net-centric” environment.

Such an environment uses a web-based infrastructure for accessing and sharing information throughout DoD for total situational awareness and superior decision making. Market-supported, open, non-government standards are becoming increasingly important for achieving the scalability and interoperability that are critical to this environment. A goal of the IT standards program is to determine which standards and products best function together to form interoperable and scalable solutions that meet DoD requirements.

Strategy

The strategy of the DoD Executive Agent for IT Standards is to increase the availability of open IT standards for DoD use in leveraging net-centric technologies and capabilities, and ensuring their widespread visibility. We must identify those groups whose activities are most closely aligned with our requirements and priorities. Unfortunately, not all SDOs or SSOs are equally effective, efficient, respected, or neutrally objective. To this end, we have developed various assessment criteria, outlined in Table 1, to provide a framework and set of objective criteria for identifying and evaluating the best candidate SDOs or SSOs for meeting our needs.

In similar fashion, we have developed some standards selection criteria, outlined in the article, “Finding the Right Standards,” to provide an objective framework for identifying the best candidate standards to include in the DoD IT Standards Registry (DISR). The IT standards governance process selects the best available standards, develops standards portfolios, and adopts them for DoD use. The approved and mandated standards and profiles are retained in the DISR.

TABLE 1. SDO/SSO Assessment Criteria

Criterion	Description
Nature of organization	Recognized authority
	Cooperative stance
	Development process
Openness	Policies on intellectual property rights
	Ownership
	User participation
	Vendor participation
Technology relevance	Leading edge
	Innovation and creativity
	Technical maturity
Stability	Participation levels
	Process maturity
	Planning horizon
Marketplace support	Acceptance
	Commercial viability
	Relevant deliveries
Usefulness/utility	Related deliverables
	Well-defined product quality attributes
	Interoperability of services and applications
Risk	Process stability
	Relevant scope
	Change management

The goal of the IT standards program is to help make well-informed decisions and leverage limited resources to maximum advantage by identifying, developing, prescribing, and implementing those IT standards that best satisfy DoD needs.

The strategy is to use accredited standards from authoritative sources in accordance with DoD policy and preferences. DoD prefers to satisfy requirements within open, consensus-based public- and private-sector standards that are currently available or under development. Being available from a reputable and authoritative source means that the responsible SDO/SSO must have an established position as an objective authority in its sphere of activity within the relevant technical, professional, and marketplace communities. This also implies that IT standards the organization develops are widely accepted and have been successfully implemented in the marketplace.

The requirement that IT standards be open is not simply a desired characteristic but based on practical legal and cost considerations. Standards must be publicly available, royalty free, and free from patents, copyrights, and other intellectual property right constraints.

By advocating incorporation of DoD requirements into open non-government, “commercial” standards, DoD encourages industry to develop and build compliant commercial products that will enable it to effectively operate in a net-centric environment.

Summary

Information and communications technology is characterized by new products, markets, and services that emerge and become obsolete far more quickly than in traditional industry sectors. Industry has long recognized that appropriate standards are essential to effective operation—indeed, to the very survival of an enterprise.

We must determine which technologies, standards, and products best function together to form interoperable and scalable solutions. Our goal is to help program and project managers make well-informed decisions and leverage limited resources to maximum advantage by identifying, developing, prescribing, and implementing IT standards that best satisfy DoD needs.

Our IT standards program provides a means to represent the requirements of warfighters and business operations in appropriate, non-government global efforts that produce market-supported, open IT standards and specifications.

Our overall strategy is to rely on the private sector to produce the needed open standards. We participate as equal partners in as many relevant external activities as we can for developing and setting standards, hoping that we have selected the right ones, based upon our comprehensive selection criteria. The purpose of our participation is twofold: to input our requirements into the standards building process and to bring back to DoD stakeholders information about trends and activities in technology standards.

The strategy recognizes that the right IT standards are key enablers to fast and accurate information awareness and exchange across the enterprise. Using the right IT standards is vital to net centrality.

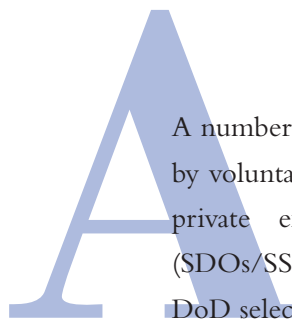
About the Author

Jerry Smith is a computer scientist in the Interoperability Standards Division of the Defense Information Systems Agency, DoD's Executive Agent for centralized life-cycle management of IT standards. Mr. Smith has more than 30 years of experience in international standards activities. ✨

DoD Representatives to Organizations for IT Standards

By Dennis Devera and Jerry Smith





A number of laws and guidelines mandate the use of technical standards developed by voluntary consensus standards bodies and require DoD to actively participate in private external standards developing and standards setting organizations (SDOs/SSOs). (See “Relevant Laws and Guidelines.”) This article outlines how DoD selects representatives to these bodies and what their responsibilities are.

Function and Selection

DoD policy is to ensure compliance with internationally accepted standards as articulated by a former Under Secretary of Defense for Acquisition, Technology and Logistics, who stated that “as DoD envisions future systems, the United States must ensure that the best people are placed on the appropriate national and international IT standards committees to convey the DoD vision and schedule, and to agree to the standards that will permit interoperability with future systems.” DoD representatives must work with relevant standards initiatives and activities to incorporate warfighter and supporting business operations requirements into market-relevant standards and drive the availability of products based on open standards.

With that in mind, selecting the right people to represent DoD interests in an external SDO/SSO is a significant task. Solicitation of interested and qualified candidates is an open process managed by the DoD Executive Agent for IT Standards. Stakeholders, military services, and agencies nominate candidates, whom the DoD Executive Agent selects using comprehensive criteria outlined in *Department of Defense (DoD) Information Technology Standards Program (ITSP) Management Plan* and “Guidance for DoD Representative Participation in External Standards Development Organizations/Standards Setting Organizations.”

Relevant Laws and Guidelines

National Technology Transfer and Advancement Act of 1995

Clinger-Cohen Act of 1996

National Defense Authorization Act for Fiscal Year 1999

National Defense Authorization Act for Fiscal Year 2003

United States Code, Title 10, Section 2223, “Information Technology: Additional Responsibilities of Chief Information Officers”

United States Code, Title 10, Chapter 145, “Cataloguing and Standardization”

Office of Management and Budget Circular A-119, “Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities”

DoD Instruction 4630.8, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”

Responsibilities

The official DoD representative is one of the most important participants in the IT standards program. This individual is the primary interface between DoD stakeholders and external SDOs/SSOs. He or she is responsible for representing the view of DoD to the designated SDO/SSO and is authorized to speak officially on behalf of DoD in that particular forum. All members of a DoD delegation to an SDO/SSO are bound by this premise: That they all will support the DoD position, provide inputs, negotiate in support of the DoD position, and vote accordingly. Table 1 summarizes the representative's responsibilities.

TABLE 1. Responsibilities of DoD IT Standards Representative

Responsibility	Description
Convey DoD vision	Convey U.S. interests in general and DoD's vision in particular—for example, Joint Vision 2020 Articulate DoD requirements Represent interests and constraints of DoD schedule Articulate and defend DoD positions
Agree	Agree to the standards that are compatible with U.S./DoD interests <ul style="list-style-type: none"> ▪ Coordinate positions ▪ Develop/submit white papers, draft technical specifications ▪ Present arguments that defend our interests ▪ Vote accordingly Take steps to help defeat actions that are inimical to our interests Defeat non-value-added proposals
Promote interoperability	Support only technical standards and specifications that will enable interoperability with DoD future systems in a net-centric environment Be alert to ferreting out those that do not
Provide feedback	Provide feedback on IT trends and activities to DoD stakeholders, especially program managers and project teams

When issues facing an SDO/SSO could result in technical requirements that may measurably affect standards significant to DoD interests, additional technical representation may be necessary to support DoD's official voting representative in dealing effectively with such situations. The composition of such delegations, in addition to the official voting representative and designated alternate, requires careful consideration. The makeup of the delegation must consider the nature and purpose of the external standards activity and the possible impact of decisions on DoD.

DoD representatives will need to integrate DoD objectives, requirements, and positions on relevant issues into the external standardization processes. Thus, they should promulgate positions or inputs to these external bodies accordingly. Where possible, the official representative uses the process described in "Guidance for DoD Representative Participation in External Standards Development Organizations/Standards Setting Organizations" to vet

and establish the official DoD position on certain IT standardization issues. (See “Principles for Working Effectively with External SDOs/SSOs.”)

PROVIDE TIMELY FEEDBACK

Stakeholders must be kept informed of significant technical and policy developments that occur during SDO/SSO activities. Official voting representatives are responsible for facilitating communication or coordination of proposals for new or modified standards throughout the organization and elsewhere in DoD where stakeholders and affected parties need to know about the issues.

MAINTAIN RECORDS

Official DoD representatives need to prepare thorough, yet concise, meeting reports; follow up with appropriate staff or stakeholder representatives; analyze issues; and distribute reports. They also should maintain a file of SDO/SSO-related information, including the procedures, bylaws, membership lists, final ballots, relevant correspondence, and minutes of meetings. A web-based SDO/SSO Collaboration Tool has been developed to support the official DoD representatives in maintaining and disseminating SDO/SSO-related information.

Summary

DoD personnel are encouraged to participate in private-sector IT standardization activities to promote standards that meet the needs of warfighters and related business operations. The official DoD representatives and their alternates appointed to external SDOs/SSOs ensure that the organizations meet DoD interests by constructively influencing the content and direction of IT standards development. Today, more than ever, influencing open standards that maintain, affirm, and uphold technology transition into market-supported defense “products” is of paramount importance in fostering the DoD transformation toward net centricity, scalability, and battlefield interoperability.

About the Authors

Dennis Devera and Jerry Smith are computer scientists in the Interoperability Standards Division of the Defense Information Systems Agency, coordinating DoD’s participation in global private-sector IT.✱

Principles for Working Effectively with External SDOs/SSOs

Work with Principal Staff Assistants, services, combatant commands, and agencies to gather, consolidate, and coordinate requirements for specific technical standards.

Advocate DoD standards requirements and positions in the appropriate SDO/SSO, and represent DoD interests in non-government standards bodies.

Form global alliances and partnerships of mutual interest among industry, consortia, professional societies, academia, and non-government standards bodies to improve availability of non-proprietary commercial off-the-shelf products that implement open standards.

Provide leadership in appropriate private-sector SDOs/SSOs to leverage promotion of DoD interests.

Replicate successful standardization projects that incorporate proven best practices.

Influence the development and adoption of standards that support DoD requirements by both the private sector and our allies.

Leverage and exploit industry standardization initiatives to maximize mutual opportunities and satisfy DoD warfighter and business operations requirements.

Foster collaboration among professional societies, industry associations, user groups, consortia, and academia to reduce fragmentation and duplication of standardization activities.

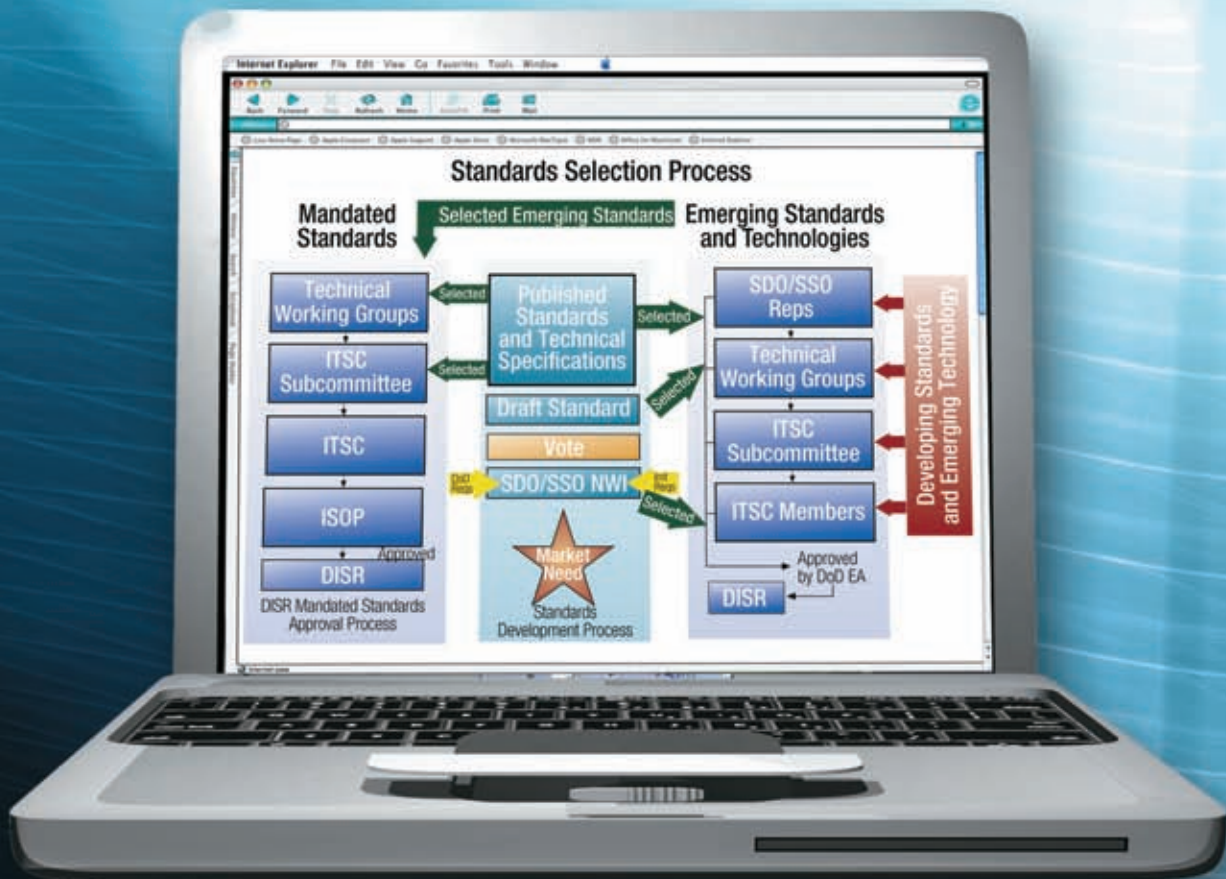
Be alert to opportunities for using seed funding to accelerate promising external standards activities that serve DoD interests and are key components for net centricity and interoperability.

Promote the use of mandated and adopted internationally accredited standards and specifications in specific DoD programs and projects by providing direct support as needed to program, project, and functional managers.

Bring back and insert IT technology, and awareness of related standards trends, into DoD priority programs and DoD engineering support activities.

DoD IT Standards Registry

By Doris Bernardini and Ken Dolson



The DoD IT Standards Registry (DISR) is the official registry of IT standards for DoD use. The secretariat of the Information Technology Standards Committee (ITSC) maintains the currency of IT standards information on the web-based tool, DISRonline, and ensures that standards portfolios are established, up to date, and reviewed. The ITSC secretariat is also the principal point of contact for coordinating standards portfolios with working groups and committees external to the purview of the DoD Executive Agent (EA) for IT Standards. The screen on page 38 shows how standards are brought into the DISR from standards developing organizations (SDOs) and standards setting organizations (SSOs).

Information Technology Standards

DoD uses IT standards from a variety of sources. These IT standards include international standards (for example, ISO and International Electrotechnical Commission), specifications, profiles, protocols, implementation conventions, Federal Information Processing Standards, military standards, defense performance specifications, NATO standardization agreements, allied communications publications, allied data publications, guidelines, commercial item descriptions, standardized drawings, handbooks, manuals, tools, and other documents relevant to the application and use of information and communications technology. In addition, DoD uses IT standards produced as non-government national standards (American National Standards Institute), consortia specifications (World Wide Web Consortium, Organization for the Advancement of Structured Information Standards), and trade association and professional society standards (Government Electronics and Information Association, Institute of Electrical and Electronics Engineers).

DISRonline

DISR is hosted on DISRonline, which also hosts other related standards guidance and direction. DISRonline includes software and hardware standards that are used for intelligence collections, data and information processing, information transfer, and information presentation and dissemination. DISRonline provides technical definitions for information system processes, procedures, practices, operations, services, interfaces, connectivity, interoperability, information formats, information content, interchange, and transmission of transfer and IT standards that apply during the development, testing, fielding, enhancement, and life-cycle maintenance of DoD information systems.

Selection Criteria

Selection of the correct standards based on appropriate technology will help enable DoD to transform to a net-centric environment and facilitate interoperability. The role of the Executive Agent for IT Standards is to identify and assess emerging technologies, manage DoD participation in external SDOs and SSOs, develop and maintain IT standards, and manage the life cycle of IT standards for DoD.

The EA uses standards selection criteria as the framework for determining which standards should be selected for inclusion in DISR. The criteria also provide guidance for moving through the DISR standards life cycle that changes the category of a standard from “emerging” to “mandated” to “mandated sunset” to “inactive/retired.”¹

The term “IT standard” as used here also includes profiles (system or IT), which are a collection of standards, parts of standards, or options within a standard by name and version, prior to emerging profiles or after becoming a reference implementation or mandated profile. Each IT profile contains one or more standards from the DISR. A system profile is a collection of one or more IT profiles.

Standard Classification Categories

Once a standard is selected, it should be categorized either “emerging” or “mandated.” A mandated standard may be reclassified as “mandated sunset” or “inactive/retired.” The current standard classification categories are defined below.

EMERGING STANDARDS

Emerging standards and technologies include

- emerging or developing technology,
- standards and specifications under development (new work items),
- draft standards, and
- candidate published standards (approved published standards by an authoritative source that are publicly available).

Emerging standards and technologies are candidates to assist DoD with tracking new technologies, new work items, draft standards, and other items or subject matter that may be of interest. Standards and technologies included in DISR should be properly classified by net-centric areas and identified as either a standard or a technology. Use of an emerging standard requires a waiver, including a risk assessment, until that standard is vetted and designated as mandated or mandated sunset.

Emerging standards include candidate published standards that help the program manager determine areas likely to change, creating a concern for upgradability. Emerging candidate published standards may be implemented, but may not be used in lieu of a mandated standard. A candidate published standard is expected to be elevated to mandatory status within 3 years. Those that continue in an emerging status for longer than 3 years require justification. Table 1 provides a notional view of the process.

TABLE 1. Process for Emerging Standards and Technology

Technology and standards of interest	Steps required	Activities	Benefits
One or more emerging technologies of interest to a net-centric environment	Select the best and most promising technologies for a DoD mission area or net-centric environment	Review selected standards development progress periodically	Continued improvement in quantity and quality of DISR standards
One or more standards being developed that should be monitored	Select the best and most promising standards for a technology area	Track selected technology trends and standards development within the technology area	Early identification of potential standards and technology
One or more draft or published candidate standards of interest	Select standards that are relevant to technologies of interest	Select published candidate standards for elevation to “mandated” or removal	Interoperability and cost savings Facilitation of transformation to a net-centric environment

MANDATED STANDARDS

Mandated standards are essential for enabling interoperability or net-centric services across the Global Information Grid (GIG). They are the minimum set of essential standards for the acquisition and development of all DoD systems that produce, use, or exchange information and, when implemented, facilitate the flow of information in support of the warfighter and supporting business operations. These standards are mandated for the management, development, and acquisition of new or improved systems throughout DoD. Mandated standards must be published (either in print or electronically) by an authoritative source.

A mandated standard may also be directed by DoD policy documents signed by an Assistant Deputy Under Secretary of Defense or higher. These policy documents usually take the form of a DoD memorandum, instruction, or manual. In such cases,

the EA, in consultation with the ITSC, should be afforded the opportunity to comment on the proposed mandated standard.

MANDATED SUNSET STANDARDS

A mandated sunset standard is a mandated standard with a predefined event and date when it should be moved to inactive/retired status. The Assistant Secretary of Defense for Networks and Information Integration is responsible for assigning a sunset tag to a standard. The sunset tag requires a waiver request with a risk assessment that includes a migration plan. A migration plan is required to explain how the system will transition from that standard when it is retired.

INACTIVE/RETIRED STANDARDS

The EA, in coordination with the ITSC, approves the designation of a standard as inactive/retired. Inactive/retired standards should not be used in a new or upgraded system. All inactive/retired standards remain in the DISR. However, when selected for inclusion in a technical standards view, an inactive/retired standard requires the previously described waiver.

Profiles

Profiles (system or IT) are a collection of standards, parts of standards, or options within a standard by name and version, prior to becoming a reference implementation, that is, implemented or instantiated. Standards must be in the DISR in order to create a profile. Each IT profile contains one or more standards from the DISR.

A system profile is a collection of one or more IT profiles. Building a system profile is an iterative process; most systems will contain more than one IT profile. IT profiles can be built by using any of the five profile-building methods in DISRonline. System engineers will often use several of these methods to construct their system profiles.

A profile may be mandated such as a key profile (KP), or may be a specific profile built to satisfy the requirements of a system or program manager, a community of interest, or a functional area such as logistics. Specific profiles may include emerging standards from DISR. A mandated profile may contain only mandated standards from DISR.

Key interfaces are functional and physical characteristics that exist at common boundaries with co-functioning items, systems, equipment, software, and data. GIG KPs provide a net-centric-oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces. KPs are a mechanism

to manage the complex interfaces within the GIG system of systems. A KP is a set of documentation produced as a result of interface analysis that

- designates an interface as key;
- analyzes the interface to understand its architectural interoperability, test, and configuration management characteristics; and
- documents those characteristics in conjunction with solution sets for issues identified during the analysis.

Managing key interfaces to ensure interoperability is critical. A single interface specification is easier to develop, implement, maintain, and enforce than maintaining synchronization of the individual interfaces of numerous systems. The approach is more legacy tolerant since it does not always assume or require changes to the internals of related systems. The approach is also system evolution tolerant; system internals can be changed, capabilities enhanced, and new technologies incorporated, as long as the interface remains stable or evolves in a measured way consistent with a defined configuration management process.

Summary

Selection of the right standards for inclusion in the DISR is only the beginning. Standards are of little use if not implemented in interfacing systems. A successful IT standard is a widely accepted specification of how to implement a set of technologies that must exchange data and interoperate. But it is what is done with that specification—how it is implemented—that measures the true success of a standard. The main goal is to facilitate transformation to a net-centric environment and foster DoD-wide interoperability and scalability.

¹The criteria that the ITSC uses is described in another article in this issue of the *Journal*, “Finding the Right Standards” by Dave Brown and Jerry Smith.

About the Authors

Dr. Doris Bernardini is a computer specialist in the DISA Standards Engineering Branch of the Interface Standards Division where she leads the DISR Support Team.

Ken Dolson, who recently retired after a long career of government service, was instrumental in revitalizing the DoD IT standards program and a key architect of the DISR. ✨

The SDO/SSO Collaboration Tool

By Robert Kidwell, Joe Brazy, Chris Kreiler, and Nonna Bond



DoD monitors or participates in numerous standards developing organizations (SDOs) and standards setting organizations (SSOs). In FY06, DoD purchased memberships in 38 separate SDOs/SSOs. Most of these organizations have subcommittees, working groups, or technical teams, each of which has one or more standards development projects underway.

Managing DoD membership in the various SDOs and SSOs has proved to be a formidable task. Management activities include annually surveying needs, tracking SDO/SSO membership accounting and financial information, managing SDO/SSO representatives and alternates, identifying key issues, collaborating with key SDO/SSO stakeholders, and developing DoD guidance packages. One of the tools used to help manage these activities was the “SDO/SSO Notebook,” a Microsoft Word document, prepared for the DoD Executive Agent for IT Standards, which contained relevant management and technical information on each SDO/SSO. The notebook contained many summary views of the information, with considerable redundancy. The maintenance of this information, when a new SDO/SSO representative was assigned, had become burdensome as the document grew to more than 1,000 pages.

Another challenge has been communicating with SDO/SSO representatives. Many representatives are tasked as an additional duty to their primary responsibilities, so their SDO/SSO membership participation is time constrained. Although e-mail provided a vastly improved method of communication between SDO/SSO representatives and stakeholders, it still only automated a part of the SDO/SSO participation process.

This situation provided the impetus to find an alternative approach to making the SDO/SSO membership management and operational tasks more efficient. The solution adopted was a database-driven web-based SDO/SSO Collaboration Tool. This tool supports an improved process for the Executive Agent’s management of memberships in non-government SDO/SSOs, and it provides DoD SDO/SSO representatives, stakeholders, and the Information Technology Standards Committee (ITSC) Technical Working Groups (TWGs) the means to collaborate, develop DoD consensus positions on key issues (via a guidance package), and share information. The tool also enables information sharing with other interested parties, as long as they have Internet access.

The specific goals for the SDO/SSO Collaboration Tool are as follows:

- Facilitate Executive Agent management of DoD’s external SDO/SSO memberships

DoD SDO/SSO 2006 Memberships

Accredited Standards Committee X12

Alliance for Telecommunications Industry Solutions

American National Standards Institute

American Society for Testing and Materials International

Biometric API Consortium

Biometric Consortium

Distributed Management Task Force

Electronic Commerce Code Management Association

Free Standards Group

Global Grid Forum

Health Level Seven, Inc.

High Frequency Radio Industry Association

Institute of Electrical and Electronics Engineers—Standards Association

International Committee for Information Technology Standards

International Federation of Standards Users

International Organization for Standardization and International Electrotechnical Commission

International Telecommunications Union—Radio Sector

- Serve as a tool for managing the activities of the DoD SDO/SSO memberships
- Provide a one-stop source of information on all DoD SDO/SSO activities
- Complement the DoD IT Standards Registry (DISR) and Defense Standardization Program Office (DSPO)
- Provide collaboration, information-sharing, and SDO/SSO management support not available at DISRonline and ASSIST-Online
- List standards developed by DoD SDO/SSO membership organizations
- Provide links to DSPO and DISRonline and other related sites.

Capabilities

The SDO/SSO Collaboration Tool is a collaborative and information-sharing web space, currently under development, to support for SDO/SSO representatives, DoD stakeholders, and other authorized users with an interest in or responsibilities related to IT standards. Figure 1 (see page 49) depicts the tool's capabilities. The SDO/SSO representative is the central actor in this environment with the capability to manage SDO/SSO information, SDO/SSO meeting-related information, SDO/SSO news, and the stakeholders. SDO/SSO stakeholders participate in issue discussions and identify and assess requirements. All users can benefit from the use of collaboration and information-sharing tools such as discussion boards, e-mail exploders list, action items, and document repositories.

Table 1 (see page 52) lists the tool's collaboration capabilities and, for each, identifies key features and related benefits to SDO/SSO users. These tools enable the SDO/SSO representatives to communicate effectively with stakeholders and keep interested parties apprised of the SDO/SSO activities.

The SDO/SSO Collaboration Tool enables the SDO/SSO representative to share vital information, both management and technical, on SDO/SSO activities and their status. SDO/SSO stakeholders can access this detailed and pertinent information at any time. Initial information-sharing capabilities, summarized in Table 2, identify key features and benefits to SDO/SSO Collaboration Tool users and SDO/SSO stakeholders.

The “SDO/SSO Notebook” contained a complete summary of relevant information about the SDOs/SSOs, their external interactions, the products they develop, and information relevant to the DoD membership management. Table 3 lists information areas covered in the notebook and indicates whether the information is primarily management or technical.

Architecture Design

The SDO/SSO Collaboration Tool architecture design features a flexible, extensible role-based collection of privileges or rights for managing the content of web pages, as well as the fine-grained control over collaboration tools. The overall architecture is divided into three major areas: a public area (no registration required), a private area (registration, user identifier, and user password required), and an administrative area, as shown in Figure 2.

Implementation views of these three SDO/SSO Collaboration Tool areas are shown in Figures 3 through 5. In addition, Figure 6 provides an SDO/SSO representative view of a part of the InterNational Committee for Information Technology Standards (INCITS) SDO/SSO information area. The blue arrow in Figure 6 points to a horizontal navigation bar with some of the collaboration and information-sharing tools, including INCITS SDO/SSO News, Syndicated News, Discussion Board, Action Items, and Document Repository.

The SDO/SSO Collaboration Tool provides for role-based user views. The information displayed and the administrative privileges are based on a user’s role. A user may be assigned one or more roles, and the roles may be tailored for unique situations. Table 4 defines the initial SDO/SSO user roles.

The public area includes a wide variety of content, including “SDO/SSO Notebook” information (except membership fee information and personal contact information). The “SDO/SSO Notebook” information and other related information are portrayed in an SDO/SSO domain model, which is shown in Figure 7. For ease in reading any taxonomy, a glossary is linked to key terms. Clicking the link will provide the glossary definitions for the selected term. Taxonomies are used to classify and link each SDO/SSO to an area of interest. Similarly, Figure 8 provides a domain model for the private area of the SDO/SSO Collaboration Tool.

DoD SDO/SSO 2006 Memberships, cont.

International Telecommunications Union—Telecommunications Sector

Internet Protocol Detail Record Organization

Internet Society/Internet Engineering Task Force

ISO/IEC JTC1/SC31, Automatic Identification and Data Capture Techniques

Liberty Alliance Project

Memorandum of Understanding/Management Group (IEC/ISO/ITU/UNECE)

MFA Forum (MPLS Forum/Frame Relay Alliance)

National Information Standards Organization

Network Centric Operations Industry Consortium

Four major technologies are used in SDO/SSO Collaboration Tool implementation:

- ColdFusion Application Server MX 7
- Oracle 10g Relational Database Management System
- Microsoft Windows Server 2003 Operating System
- Secure Sockets Layer and Public Key Infrastructure.

Access and privileges can be managed through established role-based groups. The DoD SDO/SSO official voting representatives are given maximum authority to manage within their SDO/SSO area and can approve stakeholders and update the SDO/SSO Collaboration Tool's private-side information. The SDO/SSO Collaboration Tool provides an easy method to maintain an environment for disseminating SDO/SSO information and issues that affect DoD.

Summary

The SDO/SSO Collaboration Tool will facilitate the management of DoD memberships in external SDOs and SSOs. It will enable communication of SDO/SSO issues and activities within the DoD community, as well as any selected non-DoD individuals or organizations.

Keeping stakeholders informed and involved in developing standards by providing an environment for the free exchange of ideas will greatly enhance DoD's ability to reach consensus on important SDO/SSO issues. In short, because of the tool's flexible design and the delegation of administrative privileges to the lowest level, the SDO/SSO official voting representative can more effectively participate in SDO/SSO activities.

About the Authors

Robert Kidwell, Joe Brazy, and Chris Kreiler are part of the Enterprise Integration Center (e-IC) of ManTech International Corporation. Mr. Kidwell serves as the vice president and senior technical director of the e-IC. His career spans some 30 years as a senior program manager with emphasis on enterprise-wide system integration, technical and cost issues, live test demonstrations, business process engineering, computer hardware evaluations, software engineering, and computer system performance and modeling. Mr. Brazy is the senior systems engineer of the e-IC. He served as the chief engineer for the development of the SDO/SSO Collaboration Tool. Mr. Kreiler serves as a management director of the e-IC. He developed the content of the SDO/SSO Collaboration Tool and assists the DoD Executive Agent for IT Standards with the management of DoD memberships in SDOs/SSOs.

Nonna Bond is on the staff of the Deputy Under Secretary of Defense for Logistics and Materiel Readiness/Resource Management. Ms. Bond is active in the Defense Logistics Enterprise Services Program and serves as the deputy secretary for ISO Technical Committee 184, Subcommittee 4, Industrial Automation Systems and Integration/Industrial Data.✻

FIGURE 1. Tool Support of SDO/SSO Representatives, Stakeholders, and Others in IT Standards

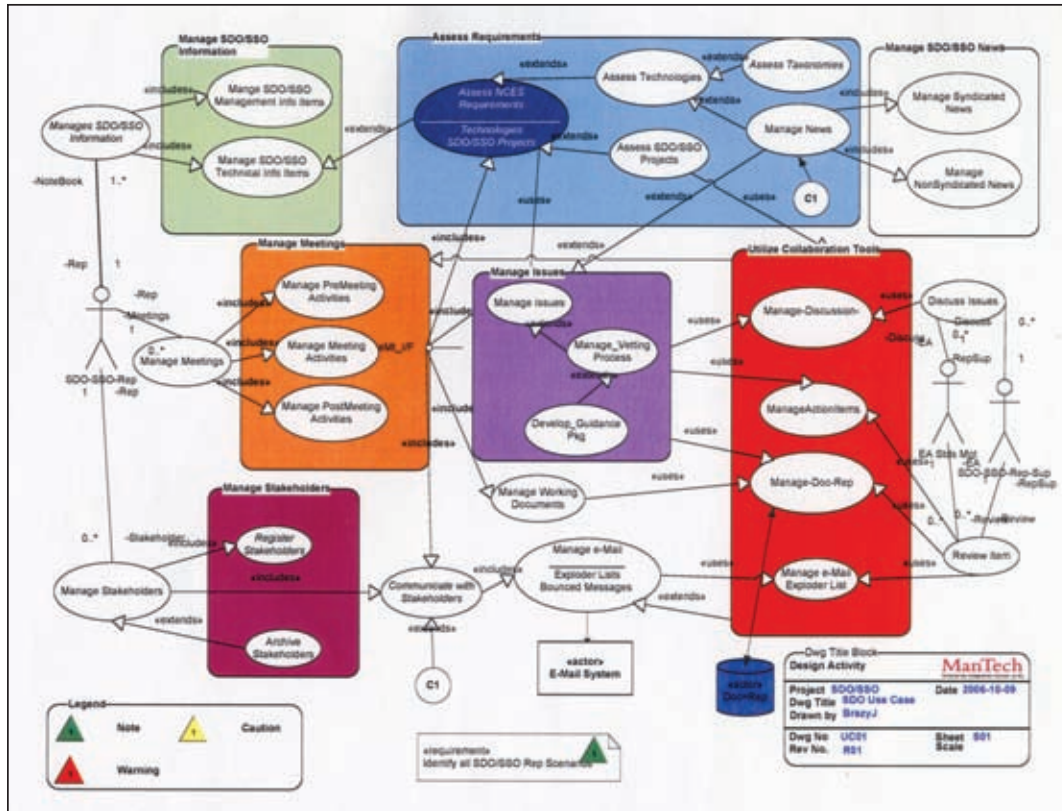


FIGURE 2. Role-Based Architecture Design

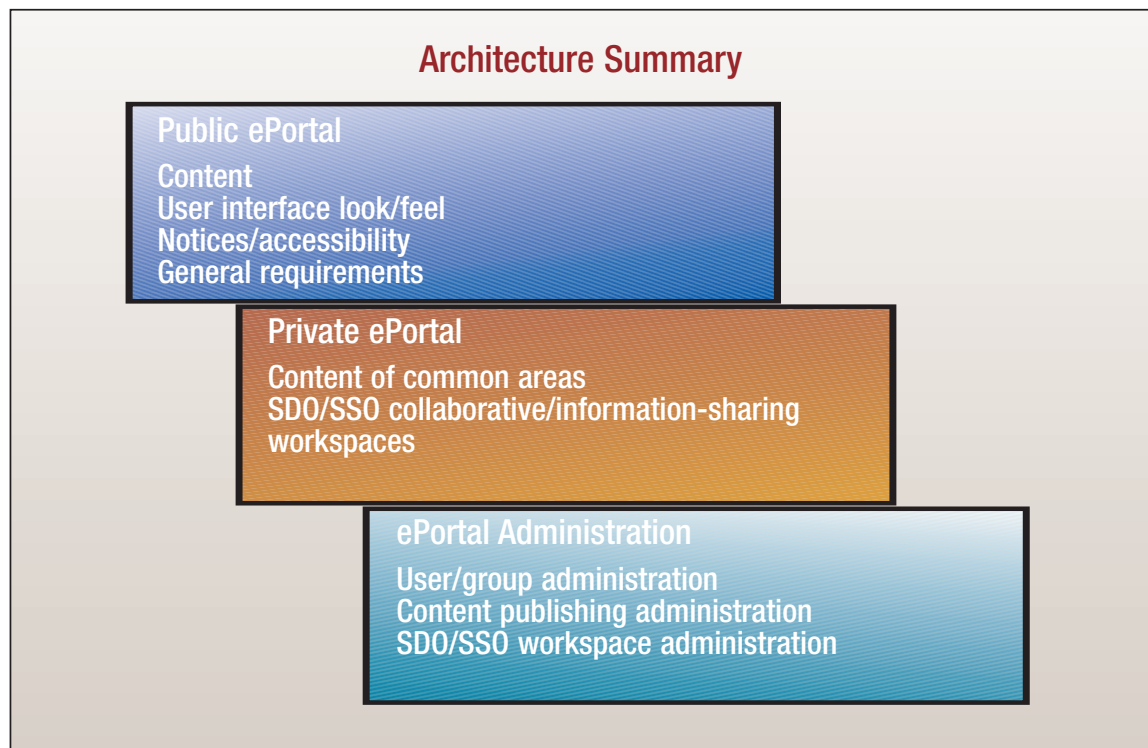


FIGURE 3. SDO/SSO Collaboration Tool: Public ePortal



FIGURE 4. SDO/SSO Collaboration Tool: Private ePortal



FIGURE 5. SDO/SSO Collaboration Tool: ePortal Administration



FIGURE 6. SDO/SSO Collaboration Tool: Representative View of Information Area

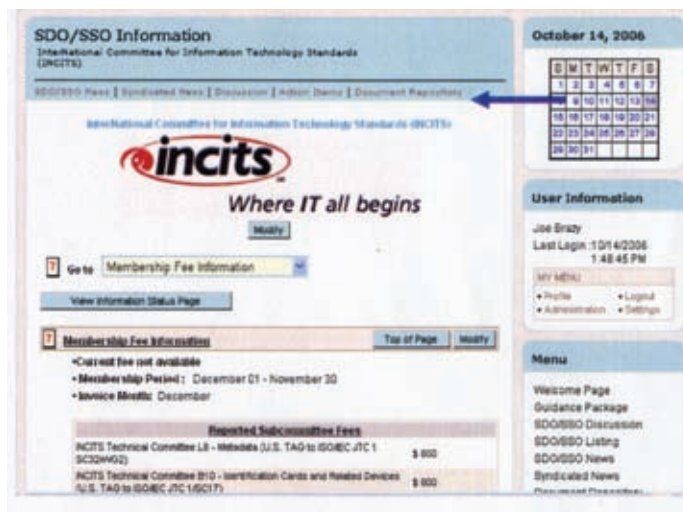


FIGURE 7. SDO/SSO Domain Model—Public Area

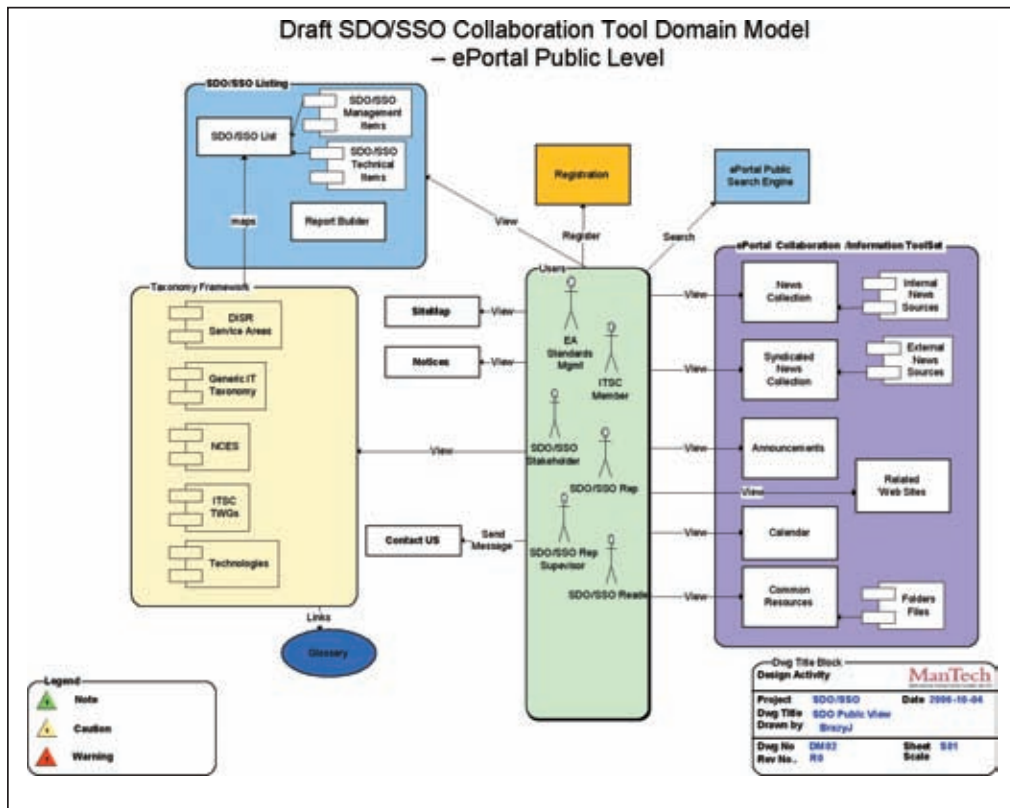


FIGURE 8. SDO/SSO Domain Model—Private Area

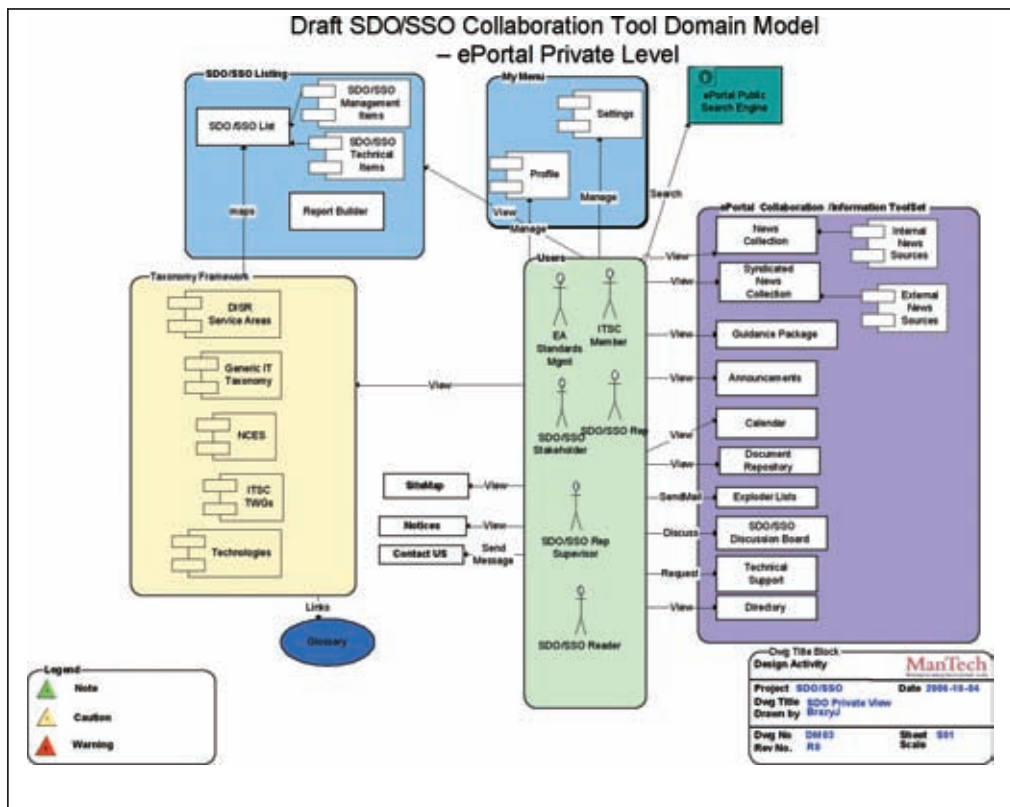


TABLE 1. Features and Benefits of Collaboration Capabilities

Capability	Feature	Benefit
E-mail exploder list	Is database driven Is extensible Is available to all registered users Supports attachments	Easier maintenance by administrator Additional exploder lists easily created by administrator Easy document distribution along with message
Hot topic issue vetting	Identifies issues Allows for comments (by stakeholders, SDO/SSO representative supervisor) Supports voting (by stakeholders)	Easier visibility of key issues and consensus for guidance packages
Calendar of events	Highlights meetings, workshops, conferences, and activities	Better visibility of events
Announcements	Highlights key events, standard development milestones, and SDO/SSO Collaboration Tool status	Better visibility of key events
Action items	Is flexible, customized to each SDO/SSO needs Supports attachments Allows for archiving	Better visibility of before- and after-meeting actions, and accessible to all authorized users Ability to support information attached to any action item
Discussion board	Is topic oriented Is persistent Supports attachments	Additional tool to discuss issues and share points of view

TABLE 2. Features and Benefits of Information-Sharing Capabilities

Capability	Feature	Benefit
DoD SDO/SSO memberships	Maintains list of current memberships Provides SDO/SSO taxonomy relationships	Better visibility of relevance to net-centric enterprise services and ITSC TWGs
SDO/SSO management information	See Table 1	Better visibility into financial information, DoD mission relevance
SDO/SSO technical information	See Table 1	Better visibility into publications, dawning technologies, technology thrusts, hot spots
SDO/SSO report generation	Provides standard reports Provides ad hoc reports	Faster report generation Flexible custom reporting
SDO/SSO document repository	Has folder/file structure Has links Has search engine Is extensible Has flexible user-defined structure	SDO/SSO representative-controlled library (enables customization to meet individual needs) Easier to locate information with search engine Flexibility to add file or links to internal or external web pages
Common resources	Is extensible Supports attachments Allows remote content publication	Better sharing of documents needed by all SDO/SSO users Easier web page maintenance by authorized administrator
Syndicated news aggregation	Provides syndicated news from external SDOs/SSOs and other IT-related sites Provides standards-based syndication	Better visibility into significant events occurring on other SDO/SSO Collaboration Tools
SDO/SSO Collaboration Tool search engine	Allows full text search and basic search Allows advanced search	Easier to find information
Directory	Provides directory of site users Provides directory of SDO/SSO members Provides directory of DoD and contractor organizations	Faster way to find contact information about users and organizations

TABLE 3. “SDO/SSO Notebook” Information

Area	Management	Technical
Membership fee information	●	
List of current representatives	●	
List of current stakeholders	●	
SDO/SSO membership information	●	
List of subcommittees	●	
List of liaisons	●	
List of issues		●
Taxonomy relationships		●
SDO/SSO description/scope of work		●
Organization membership contact information	●	
DoD mission relevance (justification)	●	
Net-centric priority rating	●	
Fora category information	●	
Deliverables/achievable objectives		●
IT publications summary		●
IT publications		●
Official DoD tasking	●	
Technology thrusts		●
Hot spots		●
Dawning technologies		●
Capabilities provided		●
Net-centric area	●	
Net-centric area relevance	●	
DoD requirements inclusion		●
DoD unique requirements needed		●
DISR profile/life-cycle code	●	
DoD leadership resource mix	●	
Costs	●	
Meetings	●	
Impact of DoD not participating	●	
External funding availability	●	
Supporting and related fora	●	
DoD stakeholders	●	
Assessment criteria	●	
Additional comments	●	●

TABLE 4. Summary of SDO/SSO Collaboration Tool User Roles

Role	Definition/Responsibilities
Super-administrator	Responsible for the overall administration of the ePortal. The super-administrator has all privileges for the website.
DoD Executive Agent for IT Standards	Responsible for IT standards management.
Information Technology Standards Committee	Responsible for reviewing the work of the ITSC subcommittees, adjudicating issues, and forwarding recommendations to the IT Standards Oversight Panel. Members of the ITSC are appointed by their respective organizations.
SDO/SSO administrator	Responsible for representing DoD in SDOs and SSOs. These representatives and alternates are appointed by letter. Additional representatives may be appointed for each SDO/SSO subcommittee or work group. Representatives are given administrative privileges solely within their SDO/SSO domain. An individual may have responsibilities in multiple SDOs/SSOs. Privileges follow a hierarchy in that representatives for the overarching SDO/SSO also have the same privileges for all subcommittees and work groups.
SDO/SSO stakeholder	Responsible for participating in the vetting process for the DoD position, which is established before issues come to a vote. Stakeholders include parties with a vested interest in the standards developed by a specific SDO/SSO. Stakeholders belong to a specific group that is associated with an SDO/SSO, subcommittee, or work group.
SDO/SSO representative supervisor	Members serve as the supervisors of SDO/SSO-designated representatives. This role is given appropriate access to function as a limited backup if the SDO/SSO representative is unavailable.
SDO/SSO readers	All DoD, contractors, and other personnel registered for access to the private area. This role has the lowest level of privileges and is limited to read only. They do not have access to the SDO/SSO vetting process.

Harvesting

Creating an ISO Standard from a Military Specification

By Nonna Bond and Chris Kreiler



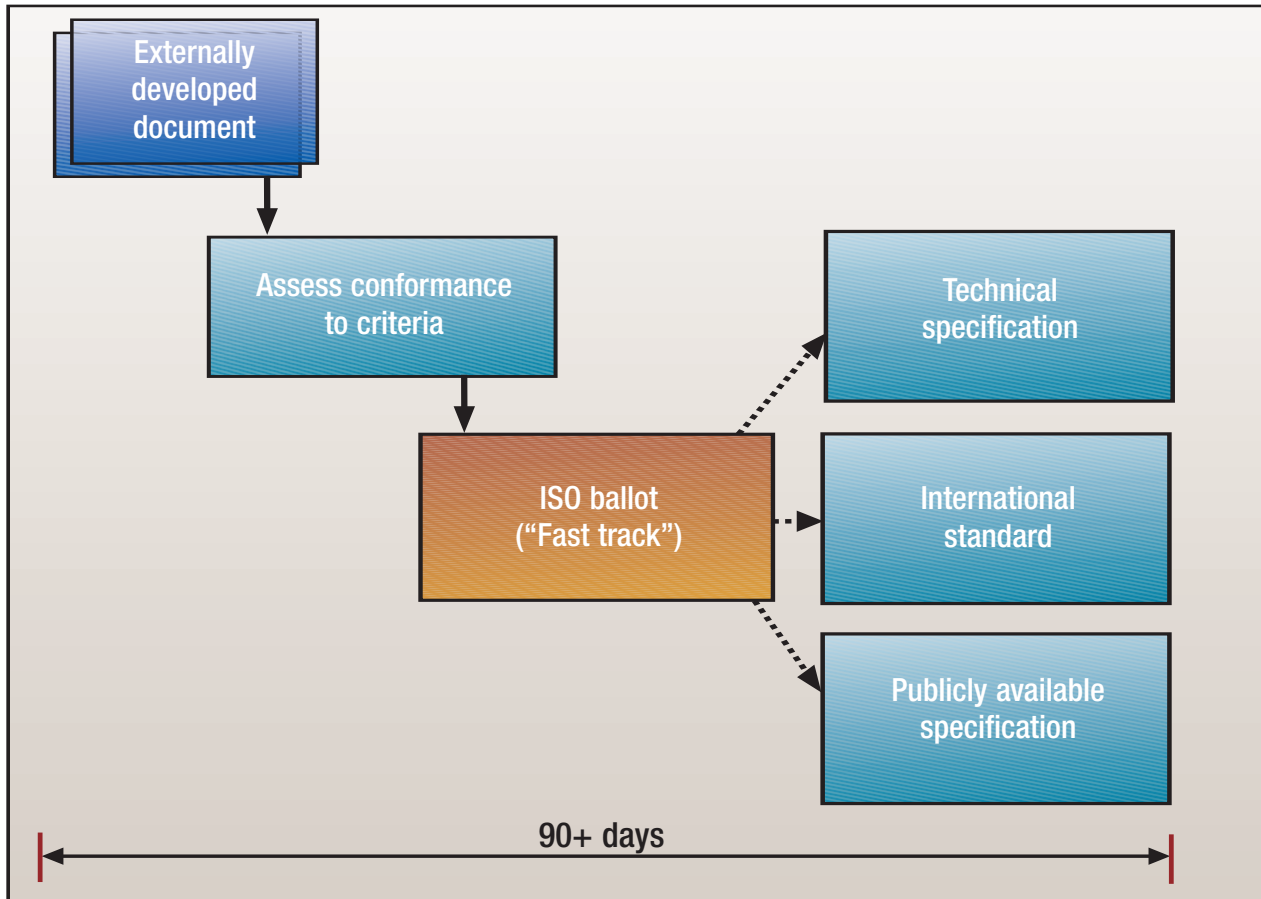
DoD needs to be able to transpose military standards and specifications into internationally recognized, accredited, and accepted documents. One way of doing this is to use the “harvesting” process available within ISO, which is considered to be the premier worldwide body for global standards.

Subcommittee (SC) 4 of ISO’s Technical Committee (TC) 184 established a process for the transposition of certain qualified externally developed documents into ISO-accredited international standards, technical specifications, or publicly available specifications. This was done in recognition that industrial automation will benefit from collaborative standardization initiatives and that cooperative and joint standardization activities offer significant opportunities to produce higher quality specifications with broader global acceptance and implementation. It also acknowledges the need to consider accepting a broader class of documents from a more diverse set of sources than is currently served by the ISO standards development process for potential recognition and transposition.

The harvesting process, depicted in Figure 1, was developed in 2001 by the Secretary of SC 4 in response to the recognition that the fast-paced evolution of information and communications technologies creates new opportunities for standards-based solutions to meet the requirements of new and emerging markets. Many outside the standards community thought that the ISO processes were too unwieldy and slow to meet the needs of fast-paced technology evolution. The harvesting approach uses an accelerated process, without burdensome administrative rules, to reach outside the standards community. When first proposed, harvesting was strongly opposed by the “technical standards gurus” not wanting to “let the ‘unwashed’ contaminate the pristine process of ISO.” Fortunately, the SC 4 community’s business interests prevailed, leading to the adoption of the process.

Using the harvesting process, quality specifications created outside ISO can be brought into the global community and quickly adopted and accredited. External organizations such as consortia, professional

FIGURE 1. SC 4 “Harvesting” Process



societies, industry associations, and government agencies now have a quick and efficient mechanism for elevating certain standards and specifications to an internationally accredited status. This presents a golden opportunity for DoD.

To date, SC 4 has successfully harvested several specifications. The following are examples:

- Transposition of Air Transport Association Specification 2000, “ATA Spec 2000: E-Business Specification for Materials Management,” Chapter 9, “Automated Identification and Data Capture (AIDC),” into an international standard in collaboration with ISO TC 20/Working Group 13.
- Transposition of the International Alliance for Interpretability Industry Foundation Class (IFC) 2x platform into a publicly available specification. In addition, SC 4 initiated efforts to harmonize the next generation of IFCs with ISO 10303, “Standard for the Exchange of Product Model Data.”

- Transposition of the Open Data Services specification from the Association for Standardization of Automation and Measuring Systems and possible integration with SC 4 standards.
- Transposition of the Strategic Automotive product data Standards Industry Group’s “Product Data Quality Guidelines for the Global Automotive Industry” into an ISO publicly available specification.
- Transposition of the European Esprit Project 20496, “Systems Engineering Data Representation and Exchange Standardisation (SEDRES),” into an ISO publicly available specification: “Industrial automation systems and integration—Product data representation and exchange—Part 20542: Reference model for systems engineering.” This specification will be integrated into ISO 10303-233, “Application protocol: Systems engineering data representation.”

The transposition of DoD’s Core Architecture Data Model specification into an ISO-accredited deliverable is underway.

SC 4 has offered to make the process available to other standards setting organizations to consider for adoption in their own standards development process.¹

¹See ISO/TC 184/SC 4 document N#1198, *Procedures for Transposing Externally Developed Specifications into ISO Deliverables*, July 2001.

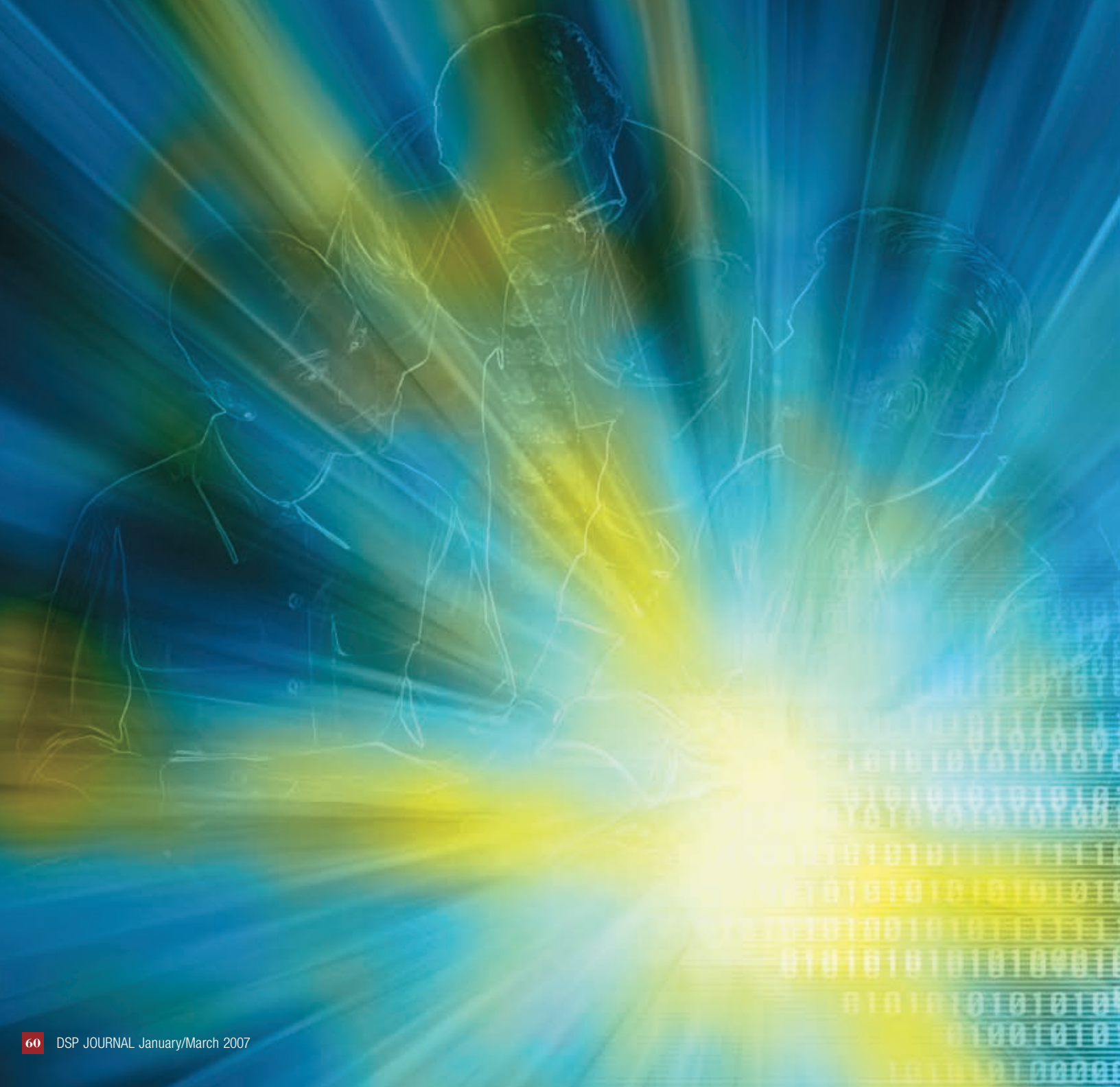
About the Authors

Nonna Bond is on the staff of the Deputy Under Secretary of Defense for Logistics and Materiel Readiness/Resource Management. Ms. Bond is active in the Defense Logistics Enterprise Services Program and serves as the deputy secretary for ISO Technical Committee 184, Subcommittee 4, Industrial Automation Systems and Integration/Industrial Data.

Chris Kreiler is a management director of ManTech Inc.’s Enterprise Integration Center. He serves as a member of the TC 184/SC 4 Secretariat staff. ✨

Lessons Learned in IT Standards Development

By Jerry Smith



After 30-plus years of experience, I've observed a few characteristics of what I consider to be “good” standards and various approaches to building them. A good standard is one thing; an efficient and effective standards development process is another. The following observations are based on some successful and some not-so-successful approaches to building consensus-based information and communications technology (ICT) standards.

Characteristics of “Good” Standards

SATISFACTION OF USER NEEDS

Good standards satisfy a universal need and are actually used. They are adequate to do the job but also exhibit quality attributes of technical excellence. They facilitate information exchange—interoperability and scalability. We see many examples of unused standards, sometimes referred to as shelf-ware.¹ We also see standards that captured the marketplace, but were, in fact, poor solutions. For example, the VHS standard is functionally and technically inferior to the Beta standard, but it won the market share war and survived. A good standard facilitates generation of relevant and useful products that satisfy needs. It solves a problem and has a certain, perceivable utility for end users.

INTEROPERABILITY

Do you recall, prior to ubiquitous wireless availability, the number of different telephone jacks needed to maintain connectivity in various locations around the world? That situation begged for global standards to foster interoperability. Borrowing a definition from the Institute of Electrical and Electronics Engineers, Inc., we need systems that implement sufficient open specifications² for interfaces, services, and supporting formats to enable properly engineered applications software that can

- be ported with minimal change across a wide range of systems,
- interoperate with other applications on local and remote systems, and
- interact with users in a style that facilitates portability.³

Interoperability contains the notion of robustness and an ability to adapt or evolve over time. The bottom line? Interoperability fosters productive interaction—exchange of resources, products, information, and ideas.

QUALITY

A good standard must be technically implementable and include all of the functionality necessary to achieve the stated level of compatibility or interoperability in a product-independent manner.

A quality standard has the following characteristics:⁴

- *Complete.* It possesses coherent functionality. Within its scope, the specification should completely describe the functionality (in terms of interfaces, protocols, formats, and so on) necessary for implementation and is an indication of how well all interfaces are specified. It includes the ease of implementation, without the need for additional descriptions, and the existence of a successful and consistent range of implementations to show its commercial viability.
- *Clear.* Contextual material is provided for better understanding by the reader. Textual and other means (tables, figures, and reference materials) are available that provide definitive descriptions. The specification is well defined and unambiguous.
- *Predictable and consistent.* It can be ported across platforms, enterprises, industry sectors, regional and national boundaries, and global entities. It is durable and long lasting, stable, can demonstrate functional coherence, and has few bugs or defects that remain unfixed.
- *Testable.* The specification contains provisions for testability. The extent, use, and availability of conformance and interoperability tests, or means of implementation verification, are described. Some form of verification (prototype testing, paper analysis, full interoperability tests) has been demonstrated. More than one vendor product has been implemented using the specification.

ACCREDITATION/BRANDING

The standard is recognized as being available from a reputable and authoritative source. The responsible standards developing organization (SDO) has an established position within the relevant technical, professional, and marketplace communities as an objective authority in its sphere of activity. To a user, this means that the specification has been created and approved, adopted, and published through a formal process, and configuration management of the specification has been established. Accreditation implies acceptance by a recognized authoritative standards setting organization (SSO). By established public law, judicial precedent, and extant policy, the U.S. government and DoD prefer using consensus-based products from a formally recognized SSO—an entity that produces and distributes formal, accredited publicly available standards.⁵ Branding is the term used by The Open Group to certify conformance.⁶ The Open Source Initiative's logo⁷ is a certification mark that indicates that the software is being distributed under a license that conforms to the open source definition.⁸

OWNERSHIP

The owner of the specification or standard is clear and unambiguous and maintains version control of the document. The owner manages changes to the document

using a formal change control process, with mechanisms to track versions, fixes, and addendums. The specification is also free of intellectual property rights (IPR) and related constraints.

OPENNESS

Standards and specifications are considered “open” when sponsored and supported by an organization that uses an open, public consensus process to develop and maintain them. This is in contrast to closed standards, which are controlled, usually as proprietary. DoD’s main issue with proprietary standards and specifications is that they promote vendor lock-in and exacerbate future legacy problems. Business enterprises, consumers, and governments alike pay dearly when locked into proprietary solutions. Table 1 summarizes the IPR issues related to open standards.

TABLE 1. Issues Related to Open Standards

Characteristics	Issues
Patents	Are there any patent rights, covering any item of a proposed specification, that the original document contributor or owner is aware of? Does the organization have written policies and procedures regarding disclosure?
Copyrights	Have any copyrights been granted relevant to the subject content of the proposed specification? What conditions, if any, apply (copyright statements, electronic labels, logos)?
Royalties	Does the organization have a published “reasonable and non-discriminatory” policy? What are the terms?
Distribution rights	What publication and distribution rights exist, and what are the terms of use? Is dual/multiple publication or distribution by other organizations possible, and if so, are there any conditions or special considerations?
Trademark rights	Will any trademarks apply to a specification? If so, what are the conditions for use? Can they be transferred in part or in their entirety?
Original contributions	What original contributions, outside IPR categories (documents, plans, research papers, tests, proposals) need consideration in terms of ownership and recognition? Will any financial considerations apply? Are there any legal considerations that apply?

Several points of view define “open” quite differently. For example, open can be defined from a process, a legal, a technical, or a user/consumer point of view.⁹ Whatever,

the point of view, openness means that participation is freely available (open) to all interested parties who are directly and materially affected; participation is not conditional upon membership in any organization, or unreasonably restricted on the basis of certain qualifications.¹⁰ Procedures governing the work of the organization are publicly available to any interested party. The process to build an open standard maintains a balance of interests. Relevant stakeholders—including commercial producers of products and services, industry-sector participants, government agencies, users, developers, testers, and researchers—all participate equally. It provides the means for multiple parties and interests to overcome conflicting interests to achieve a commonly agreed outcome. It is suggested that a metric is the degree to which competitors collectively participate and support the process and its deliverables.

By driving the incorporation of user, consumer, and business operations requirements into ICT standards, we encourage industry to develop and build commercial products using open standards. As more and more vendors offer compliant COTS products, prices go down, the number of standardized products goes up, and reliability, robustness, and interchangeability increase.

INCORPORATION IN COMMERCIAL OFF-THE-SHELF PRODUCTS

Good standards are used in building successful commercial off-the-shelf (COTS) products. From a user's perspective, it is best to have available a choice of competing conforming products. Ultimately, standards must be validated by marketplace acceptance; in other words, vendors need to produce COTS products based on open standards. As Phil Condit, a previous chairman and chief executive officer of The Boeing Company, said, "markets—not standards committees—determine which standards will be the winners!"

A successful standard is a widely accepted specification of how a set of technologies that must exchange data and interoperate need to be implemented. But it is what is done with that specification—how it is implemented—that measures the true success of a standard. By driving the incorporation of user, consumer, and business operations requirements into ICT standards, we encourage industry to develop and build commercial products using open standards. As more and more vendors offer compliant COTS products, prices go down, the number of standardized products

goes up, and reliability, robustness, and interchangeability increase. This significantly enhances interoperability. By users and consumers influencing the specification of international standards, competition to deliver required products increases while making newly developed products more marketable globally. As a result, conforming products are readily available in the marketplace. Carl Cargill, vice president of Sun Micro Systems, sums this up best: “Success of a standard is measured by the number of competing implementations that build upon that standard, not in the creation of the specification itself.” Thus one metric for determining the “goodness” of a standard is the extent of conforming implementations.

Characteristics of “Good” Development Processes

The following are some observations and conclusions with respect to management of ICT standards development and standards setting:

- *Standards vs. technology.* There is a natural tension between technology evolution and standards setting. Timing is critical. If one sets standards too early, the result is to stifle innovation and creativity (the fuel of technology evolution). Setting them too late engenders social and economic costs (as seen in Beta vs. VHS).
- *Performance vs. process.* Successful standards specify performance and interface requirements. Telling a vendor how to build a product is a poor example of how to establish effective standards. Users and consumers are interested in the final product—not the process used to get there.
- *Marketplace support.* The marketplace determines which standards are the winners. Good (effective, useful, desirable) standards allow a range of implementa-

Definitions of “Open”

“Open” can be defined in various ways, depending on the viewpoint:

- The *process* viewpoint is concerned with the ability of all stakeholders to participate in the process.
- The *legal* viewpoint is concerned with legal issues, defining open in terms of intellectual property, considering a standard to be open if it is royalty-free and unencumbered by IPR claims.
- The *technical* viewpoint focuses on whether an open standard allows for the unrestrained exchange of technical information in developing a standard.
- The viewpoint of the *user/consumer* considers the products that result from use of a standard such that the bottom line focuses mostly on the software. Thus, the concern is whether anyone, anywhere, for any purpose whatsoever, has the right to use the software, copy it, modify it, and distribute those modifications free, or for a fee, and with the right to have the actual source code that makes those things possible.

tions and are supported in the marketplace. Part of the premise is that vendors can gain a competitive edge by using open standards.

- *Relevance.* The chief end goal is widespread recognition and acceptance of standardization process deliverables—open standards that are actually being used in conforming COTS products. There seems to be a relationship between “hot” new technology and the level of consortia activities, and this metric can provide some clues about relevance. The key for users is to encourage new consortia and other SDOs/SSOs to collaborate to produce technologically current standards that vendors use in COTS products.
- *Management as a project.* A good process produces a quality technical document (specification) reflecting a business case via an engineering and management process that considers relevant user and industry input. The process needs to be requirements driven; use a proven engineering method; and be managed as a “project” with coordinated expectations, correctly applied expertise, specific deliverables, adequate resources, realistic schedules, and associated accountability.
- *Quick publication.* Specifications should be published quickly, supported by an effective means to capture defects, add new and better enhancements, and incorporate new ideas as extensions and later versions. A successful project will preclude “feature creep” and “perfectionism.”
- *User advocacy involvement and participation.* Necessary participants include all stakeholders with a material interest; these include technologists, vendors, testers, users/consumers, and government agencies, and others actively involved in setting standards. High membership fees and intensive resource investments, such as extensive face-to-face meetings requiring significant travel expenses and time away from the office, are barriers to small and medium enterprises’ participation in standardization activities.
- *Product of a consensus process.* The most useful and stable standards seem to come mostly via a voluntary consensus process. And the broader the range of consensus, the higher the quality of the resulting specification. The ICT standards principles adopted by DoD define consensus process characteristics.¹¹
- *Open deliverables.* Standards and specifications are considered open when sponsored and supported by an organization that uses an open, public consensus process to develop and maintain them. This has to do with control of the document and the absence of IPR issues. The owner of products published by the organization is clear and unambiguous and is responsible for version control. The organization developing and publishing the specification has documented policies regarding document ownership, distribution, IPR, and change control. There is a written statement that delineates the attitude of the organization and its members regarding IPR with reference to a candidate specification, for

example, patents, disclosure, copyrights, royalties, published “reasonable and non-discriminatory” policy, distribution rights, trademark rights, and original contributions.

- *Collaboration.* The process is collaborative, avoiding antagonism among various constituencies and subversion by minority interests.

In addition to emulating the above good characteristics, a viable standards development process needs to avoid some traps observed in past project failures. Unfortunately, many failures are not easily recognized until long after a project starts—sometimes years later. The following are key traps to be avoided:

- *Standards for standards sake.* We’ve all witnessed various shelf-ware standards activities that never really go anywhere. Indeed, they are actually counterproductive to the global ICT standards community’s long-term interests. When certain special interests, especially some of the small projects fostered by standards consultants and academics, obtain funding to pursue their standards-for-standards-sake technical projects—most of which are not only of highly questionable value, but more important, are invariably proven to be antithetical to global community interests—they use limited funds that are needed for better, more legitimate ICT standards activities. They are a negative and counterproductive drain on the standards community infrastructure. Little or no acceptance or use of a standardization project deliverable is a strong metric of project failure.
- *Unclear focus.* Implementations should not be standardized. Instead, the focus should be on standardizing interfaces and expected outcomes. Vendors should be encouraged to develop conforming COTS products that are differentiated by features. They should be very careful about incorporating leading-edge, new, or untried technology. Experience shows that being conservative is best in most cases. Keeping in mind who will implement the standard and who will purchase conforming products will help reduce the risk of standards for standards sake.
- *Feature creep.* Expanding a project’s original scope—adding new ideas, features, and capabilities, regardless of merit—generally proves to be a schedule killer. However, there is a real need to fix defects quickly. Experience shows that, like software, fixing bugs later is more difficult and expensive.

Our experience is that consortia are good for technology development, and the formal standards process is good for consensus building. The standards activities, professional societies, industry associations, and consortia each have a role, scope, and purpose, but they generally do not compete. Instead, each community contributes to the standardization process and a coordinated approach, based on combining the best that each community has to offer—a very effective model for standards development.

Summary

Standards and the standardization process are boring to most people:

- They do not generate high interest and excitement among engineers and technologists in general.
- Program and project managers are keenly interested in budget and schedule, but frequently view standards as obstacles.
- Most chief executive officers usually do not see standards, and their organization's participation in standardization activities, as a positive influence on the company stock price for the next quarter.
- Standardization is not considered to be a high-profile issue with politicians.
- Users are interested only in the final product and fail to appreciate the role and value of standards and the standardization process in helping them obtain interoperable products and services.

An effective ICT standardization approach needs to consider these realities.

On the surface, working with IT standards may not appear glamorous. But just as the company commander who brings his troops through a firefight intact, those of us who work with IT standards can feel a particular pride when we influence a standard that will save the lives of countless men and women we'll never know or see. With standards, we help save the tax dollars of other hard-working Americans just like us. So when we are working in the IT sector, we do our homework, establish important relationships, participate in countless groups known by myriad indecipherable abbreviations, and work hand in hand with our military and civilian counterparts, with nothing but higher standards in mind. And when we achieve them, we can all share a sense of pride and accomplishment. Even though it may not be viewed as glamorous, it's still a victory; and that's worth celebrating.

¹According to the National Center for Manufacturing, the United States has almost 100,000 published technical standards (more standards than most other nations), but a significant portion of them document obsolescent technology, are redundant, or are overlapping. An American National Standards Institute (ANSI) study showed that 80 percent of the orders for individual standards are for only 15 to 20 percent of the total number published.

²The terms “specification” and “standard” are used fairly loosely in this article. Some would say that a specification is a future standard under development and that it becomes a standard when formally published and released as such.

³Institute of Electrical and Electronics Engineers, Inc., POSIX 1003.0.

⁴This list is excerpted from ISO TC 184/SC 4 N#1198, “Procedures for Transposing Externally Developed Specifications into ISO Deliverables,” July 31, 2001.

⁵Congress prescribes management of IT and national security systems standards for DoD. Formal direction comes from several sources, including United States Code Title 10, Section 2223; Clinger-Cohen Act of 1996 (Public Law 104-113); National Technology Transfer and Advancement Act (Public Law 104-113); and various National Defense Authorization Acts. DoD standards policy is found in DoDD 5101.7, “DoD Executive Agent for Information Technology Standards,” May 2004, and related documents. These principles are based on ISO and ANSI principles and the “National Standards Strategy” published by ANSI.

⁶The Open Group has a conformance certification program for the Common Operating Environment (COE) Platform, CORBA®, Directory, LSB®, POSIX®, Schools Interoperability Framework (SIF), TOGAF, UNIX®, and Wireless Application Protocol (WAP). The Open Group developed Test Suites for UNIX, CDE, and XPG4 branding.

⁷See <http://opensource.org/trademarks/osi-certified/>.

⁸See <http://www.opensource.org/>.

⁹Larry Rosen, Panel Discussion on Legal Issues, Open Source Conference at the University of Saint Thomas, Minneapolis, MN, June 24–25, 2003.

¹⁰These properties are based on ISO and ANSI accreditation processes and procedures.

¹¹DoD IT standards principles are articulated in DoDD 5101.7, “Executive Agent for Information Technology Standards,” May 2004, and related documents. They are based on various ISO and ANSI principles and the “National Standards Strategy” published by ANSI.

About the Author

Jerry Smith is a computer scientist in the Interoperability Standards Division of the Defense Information Systems Agency and coordinates the DoD’s participation in global private-sector IT standards activities. He has served as the DoD voting representative to myriad external standards setting organizations over the past 12 years. ✨

March 13–15, 2007, Arlington, VA
*Defense Standardization Program
Outstanding Achievement Awards
Ceremony and Conference*

The Defense Standardization Program Outstanding Achievement Awards Ceremony and Conference will be held March 13–15, 2007, at the Westin Arlington Gateway Hotel in Arlington, VA. The Westin Gateway Hotel is accessible by metro and is close to National Airport, the Pentagon, and Washington, DC. Rooms will be offered at the government per diem rate.

This year's event will be administered by the Society of Automotive Engineers and promises to be top notch in every respect. Although details are still being worked out, there will be a Standardization Executive Panel, discussion of new initiatives regarding parts management, and presentations on NATO and international interoperability. Tutorials will be presented on the Berry Amendment, ITARS/EARS, RFID, updates to the DoD 4120.24-M, and much more. For more information, go to www.sae.org/events or www.dsp.dla.mil/ or call 703-767-6870.

July 10–12, 2007, Chantilly, VA
*Course on Standardization within
NATO (U.S.-Based Track)*

On July 10–12, 2007, the International Cooperation Office, Defense Standardization Program Office, and North Atlantic Treaty Organization Standardization Agency (NSA) will host the first course in the United States on Standardization within NATO. This course is designed to present an overview of domestic and international standardization practices within the United States as they relate to interoperability with allies and partners. Thus, the course is intended for military, DoD civilian, and federal government personnel who have little knowledge of international standardization or knowledge in distinct areas but have never taken the Standardization within NATO course. Non-DoD federal government employees and defense contractors who are involved in NATO standardization and interoperability activities are also eligible for this course depending on space availability.

Seats are limited, and going fast. If you're interested in attending this course, please contact Latasha Beckman at latasha.beckman@dla.mil.

August 20–21, 2007, San Francisco, CA

56th Annual SES Conference/12th International IFAN Conference

The Standards Engineering Society will hold its 2007 annual conference in conjunction with the 12th international conference of the International Federation of Standards Users. Join us for an informative and lively conference featuring representatives from around the world to discuss global standards issues. For more information, go to www.ses-standards.org or e-mail admin@ses-standards.org.

Navy Six Sigma Kaizen Event to Improve Overage Document Review Process

The Navy Departmental Standardization Office convened a 3-day six sigma kaizen event in January 2007 to improve the process by which the Navy prioritizes, evaluates, updates, and validates the overage documents for which they are responsible. The goal was to improve the way the Navy ensures the technical adequacy and currency of its specifications and standards in order to better support operations, acquisition, and logistics support. There were a number of recommendations for

changing Defense Standardization Program policies and prioritizing overage documents, but the most significant recommendation is to add a document feedback capability to ASSIST that would become a permanent, central repository for technical feedback collected for every document. Such information would be valuable in assessing the technical adequacy of documents, prioritizing workloads, and assessing whether a document needs to be updated, canceled, or validated. All of the services and agencies will be invited to participate in the technical requirements definition for this feedback system and take part of the ensuing pilot program.

Farewell

Raymond Monnin, Defense Supply Center Columbus (DSCC), OH, retired on December 31, 2006, after 20 years of federal service. Mr. Monnin started his federal service in engineering and standardization with the former Defense Electronics Supply Center (DESC), Dayton, OH, in May 1986. His accomplishments from his entry electronic engineer position at DESC to the Microelectronics Team Chief position at DSCC were many. His notable accomplishments were the development and management of the standardization program for the monolithic and hybrid microcircuits; the contributions of his engineering expertise to the Joint Electron Device Engineering Council's JC-13 Microcircuit Committee, and the Government Electronics and Information Association's G-12 Users Committee; and his tireless collaborative effort with the Defense Standardization Program Office in transitioning the Defense Microcircuit Planning Group to the DoD Joint Standardization Board on Microelectronics and Semiconductors.

Welcome

On January 9, 2007, **Kristin Stanley** was appointed as Standards Executive for the U.S. Army Materiel Systems Analysis Activity (AMSAA) at Aberdeen Proving Ground, MD. Ms. Stanley led the Research, Development and Engineering Command's Standardization Working Group to improve internal standardization processes. In addition, she actively contributed to AMSAA's standardization efforts, specifically in the development of web-based tools that will facilitate the application of Visual Growth and other AMSAA methods.

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 2007	IT Standardization
July–September 2007	DHS Standardization
October–December 2007	Parts Management

If you have ideas for articles or want more information, contact Tim Koczanski, Editor, *DSP Journal*, J-307, Defense Standardization Program Office, 8725 John J. Kingman Road, Stop 6233, Fort Belvoir, VA 22060-6221 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.

