Navigating the Enterprise Forest

Fred Smullin
Integratable Technologies, LLC

What happens when you take a local depot solution and promote it for worldwide use? You suddenly find yourself facing the challenge of integrating into the Department of Defense (DoD) enterprise with few maps to guide you. I will share my lessons learned as the former chief software architect of the G200 Defense Repair Information Logistics System (DRILS) that started as a local solution and matured into an Air Force solution used both in the .com and .mil domains.

DRILS began as a local maintenance data collection (MDC) system in 2000 to capture the serialized repair of assets. It was commissioned by F-16 supply chain managers (SCMs) to connect them in real time to depot avionics repair activities at Hill Air Force Base. The objective was to collect and analyze vital repair shop information in order to increase the reliability and availability of F-16 avionics as well as decrease repair costs [1]. DRILS most importantly facilitated documentation of individual chips, resistors, and other small parts being replaced within the aircraft avionics components. Other Air Force MDC systems were not able to provide this level of detail, which turned out to be the most important data to SCMs as these parts were the ones that actually failed within the avionics components. The information analyzed from DRILS by the F-16 SCMs under their Falcon Flex program [2] has enabled $133 million in cost avoidance since 2000 and has been projected to achieve approximately $678 million through the aircraft end of life [3].

I will admit that the DRILS stakeholders were naïve to the DoD approval requirements for an Information Technology (IT) system. It would take us more than a year after fielding our initial prototype to navigate our way and be recognized as a legitimate IT system.

The DRILS story is not unlike those of other locally grown data systems in the DoD. An information gap existed within the current mix of maintenance information systems and the depot organization took steps to plug that gap which eventually gave birth to DRILS. You do not have to look far to find information gaps in the DoD. We live in a data rich environment, yet we are information poor; someone somewhere does not have access to the information they need. This basic hunger for dependable information, as well as the lead time and funding required to modify legacy systems, leads to creation of local stovepipe solutions funded and built by the user in that domain.

Tight budgets are impacting the ability to implement local solutions. A 2004 U.S. General Accounting Office (GAO) report found that the DoD requested approximately $19 billion for fiscal year 2004 to operate, maintain, and modernize 2,274 business systems. The report also identified that uncontrolled DoD spending resulted in stovepiped and duplicative systems that included more than 200 inventory and 450 personnel systems being procured and sustained. Very often these stovepipe solutions get thrown over the wall to DoD IT organizations to integrate and sustain within the enterprise [4]. The costs of the integration and sustainment efforts result in priorities getting shifted within existing budgets to accommodate these unplanned requirements.

The National Defense Authorization Act (NDAA) of 2005 was crafted to specifically address this issue [5]. It requires the DoD comptroller to determine that system improvements exceeding $1 million meet the criteria specified in the act. DoD portfolio management (PfM) initiatives have been introduced to comply with the NDAA requirement as well as limit the flow of local solutions that may be stovepiped or duplicative. However, the door is not completely closed to approval of local systems. You can get your local solution approved to operate if you know how to navigate your way through the forest. Based on my experience, if you take the time to address the following questions, you will increase your likelihood of surviving in the enterprise.

What Gaps Are You Filling?

Identify what gaps you are filling in the information food chain. Is there a reason why no one else is providing the information? This is your critical foundation upon which everything else is built. If you are merely churning out the same information that other systems are producing, you will not get far. Focus on those information gaps that prompted you to build the system.

Take those gaps and then describe what is in it for the user community, especially the person doing data entry. Are they getting more out of it than what they put in? If it is not useful to them, you are not going to get your dependable data. Make it worthwhile for them, and you will never be short of dependable data.

Any requirement, given enough time and money, can be integrated into any legacy system. One of the most common reasons a requirement is not integrated is that few organizations have the time and/or money legacy systems request to implement a new requirement. The user community finds it cheaper and faster in the near term to implement their requirements to fill the information gap, and hope to interface it with a legacy system down the road. Unfortunately, this is counterproductive as it just creates more stovepipes.

Try to identify if legacy systems have plans to plug this information gap, and if so, when. If there are plans but they are years out on the horizon, you may get interim authority to operate your gap-filling solution that could evolve into a long-term solution if the implementation is done well.

Develop your own comparison matrix of legacy systems that perform similar functions or may potentially interface to your system. Try to be impartial in your evaluation in order to maximize its credibility. Contact the legacy systems and educate them about what you are doing. Approach them with a partnership offer that assists them with improving the quality of data and information in their system. Document which systems you would interface with if you could and why. Estimate interface costs and return on investment where possible. Interfaces to legacy systems usually provide returns on investment in the areas of duplicate data

entry reduction, minimization of data entry errors, improved data dependability, and near real-time data updates across the enterprise. Keep in mind that there are two costs to any user interface: yours and the legacy system. Your user community may have to pay for both.

In the case of DRILS, we saw that it could potentially interface with the Reliability and Maintainability Information System (REMIS) and the Core Automated Maintenance System (CAMS). Users were frustrated with data entry processes and business rules they perceived to be cumbersome as well as with challenges they encountered trying to analyze historical data. We focused our efforts on streamlining the data entry and data analysis processes for our users. On the depot shop floor, we were able to cut data entry time by 80 percent on average compared to the legacy system. The result was that the volume of depot maintenance data actually increased from the shop floor when compared to the legacy data system. Interfacing with the legacy systems turned out to be the greatest approval challenge. It took nearly six years of meetings, briefings, and requests for funding before the official system interface was allowed to be built with REMIS. A CAMS interface is still actively being pursued at this date.

One lesson learned is that headquarters is generally willing to entertain temporary solutions to initially fill information gaps. Locally developed temporary solutions are usually more agile and less costly than legacy systems to experiment with. Thus, temporary solutions are excellent proving grounds for defining requirements to be incorporated into the legacy system in the long term.

This proved true for DRILS: Our user community encompassed a relatively large portion of the F-16 avionics community but was still small when compared to Air Force-wide MDC legacy systems. Our development and support teams were also much smaller which shortened our decision-making time. The architecture design allowed us to isolate experimental modules from all user communities except those participating. Thus, our cost to implement requested changes for experimental initiatives was significantly smaller and our time to value was also significantly shorter. This made DRILS an ideal system to support MDC experiments such as Air Force Serial Number Tracking initiatives sponsored by high-level champions.

Who Are Your Champions?

A key to successfully implementing any IT system in the DoD is to identify champions within the customer and user base. Champions identified within this community can help advocate the system at the various levels of review and approval. These champions need to be evangelistic because their support will be tested up the chain of approval. They will need to be able to communicate their need and why your solution is the best.

For example, in the case of DRILS, we were fortunate that the product concept and implementation sold itself. Several levels of champions sprung up during the product implementation. The SCMs wanted the repair data from the shop floor and convinced the repair shop supervision to give it a try. Supervision asked their data entry technicians to try the system. They did with some reluctance, but once they started entering data, they became believers.

"A key to successfully implementing any IT system in the DoD is to identify champions within the customer and user base. Champions identified within this community can help advocate the system at the various levels of review and approval."

Technicians in depot repair shops are graded on their production, and the overall organization is graded on its ability to produce quality assets on schedule and on budget. Any impediment to those goals can impact their customers and cost them workload in their competitive environment. Legacy MDC systems used until then had been deemed cumbersome to use by those using it and did not provide any perceivable value to those technicians in meeting quality, budget, and schedule. The DRILS development team lived on the shop floor for nearly four years working hand in hand with the using technicians to refine how the data was collected and displayed. This enabled the system to provide immediate payback to the person entering the data.

This focus on the technician at the point of maintenance enabled them to proactively identify issues that most likely would not have been detected with the legacy systems. A real-world example involved the F-16 multi-function displays whose newly manufactured replacement power supplies that cost $5,000 each were failing within five months of installation. The DRILS design enabled the technician to easily notice the trend, stop installing those parts, and alert the SCM who triggered an investigation with the manufacturer. That investigation eventually led to the identification of a defect in the manufacturing process. Without DRILS, the trend may have gone on for many more months and possibly grounded aircraft due to failed parts clogging the supply chain and consuming financial resources.

Stories such as these enabled long-standing issues to start getting fixed. These success stories gained the attention of the warfighter customer who then wanted the system adapted for their use. This sold the supervisor who in turn sold their Colonel who in turn sold his Brigadier General. The Brigadier General then raised awareness all the way to the Office of the Secretary of Defense. Word started to spread between the weapon systems and Major Commands when warfighters who had used the system moved from unit to unit. It was not long before we had obtained several levels of champions. But our most critical level continued to be the data entry person at the point of maintenance.

How Do You Align With the Mission?

Another key to winning acceptance in the DoD enterprise is to identify how you align with the overall IT mission of your agency and the DoD in general. Obtain copies of headquarters briefings in your domain and examine their road map and the issues they are trying to solve. How do you fit within that road map? If you can show how you fit within that road map, you can gain critical awareness and possibly acceptance at the headquarters level. Part of gaining acceptance is educating them about how you fit with current legacy systems.

Compliance With Standards

The IT industry continues to evolve toward a net-centric world where standards-based computing is pushing out proprietary products in order to facilitate easier integration in heterogeneous envi-

ronments. The DoD continues to gravitate to these standards, although slower than industry, for the same reasons. It is important that you inventory applicable technology standards in your application domain as well as those of the mission you are supporting and remain consistent with those established standards.

DRILS is a Web-based Air Force maintenance data collection system; well-published standards for maintenance data existed in Technical Order 00-20-2 and other publications [6]. We had to remain consistent with those standards at a minimum in order to be able to feed data to the legacy MDC systems in order to allow a much broader Air Force audience to analyze the data. Technology-wise, we intentionally selected well-known commercial off-the-shelf products and kept those products to a minimum in order to avoid integration headaches while remaining consistent with the Global Combat Support System – Air Force requirements.

Can You Participate in a Pathfinder Initiative?

Pathfinder initiatives are very beneficial. Merriam Webster's online dictionary defines pathfinder as, "one that discovers a way; *especially*: one that explores untraversed regions to mark out a new route" [7]. My experience with pathfinder initiatives has involved a charter between a particular community of interest and the headquarters to solve a process or information gap. These pathfinders involve assembling members of the community of interest to review and improve processes and policies. In order to establish a baseline and measure the effect of change, the pathfinder members must collect data. Thus, appropriate data systems are selected as tools to provide the data.

For example, the Air Force decided to initiate a Reliability Pathfinder to study and define the benefits of Item Unique Identification and Automated Identification Technology (AIT) in regards to facilitating serial number tracking within the maintenance processes. The pathfinder team members analyzed the available data systems and chose to use DRILS as the tool with which to collect their data. They performed their analysis on selected B-52 avionics maintenance occurring on the flight line and at the depot. DRILS was used basically as is with a few minor software modifications to facilitate specific data collection and analysis. The result is that the Air Force Reliability Pathfinder has proven very successful. Reports are currently being prepared that have the potential to positively impact the future of serialized asset tracking.

What I learned while participating in three Air Force and two joint Air Force and Army service pathfinder initiatives is that they are useful for unifying a vision. Headquarters depends on field users to define requirements for them. Users want headquarters to make decisions and investments that will improve their work environment, but often do not know how to effectively communicate requirements. I saw disconnects occurring on both sides.

"A pathfinder initiative provides an excellent forum ... to collaborate in a closed environment, reach a common understanding, solve longstanding issues, and communicate those solutions to all parties. If you can team with an existing legacy system ... then you have significantly increased your odds of being approved."

A disconnect may occur in the understanding of the big picture at the user level, while the headquarters may not completely understand the detailed needs of the user. A pathfinder initiative provides an excellent forum for these two groups to collaborate in a closed environment, reach a common understanding, solve longstanding issues, and communicate those solutions to all parties.

To participate in a pathfinder, you need to apply your gap assessment, the backing and breadth of your champions, and your legacy system comparisons to make your case to headquarters of how you can help with a pathfinder effort. If you can team with an existing legacy system to solve the pathfinder needs, then you have significantly increased your odds of being approved.

Pathfinder efforts are as resource-challenged as any other program. Therefore, financial resources to support your efforts will be very limited. However, the exposure and lessons learned from a successful pathfinder effort are significant. Pathfinder progress reports are reviewed at the highest management levels. A successful pathfinder effort will often lead to other pathfinders that increase the exposure of your system as well as your acceptance within the DoD IT community.

Do You Have Portal Capability?

How many user names and passwords do you currently maintain? Do you think users will be willing to add your system to the list as well? I am personally aware of an office that did a Lean study and found they lost 1.5 hours of productivity per day logging in and out of 22 data systems to do their job. This frustrated the workers and decreased their overall job satisfaction.

You can increase your probability of user acceptance by checking to see if there is a portal such as the Air Force Portal or Army Knowledge Online (AKO) that you can integrate with to provide streamlined sign-on capability. Check with your portal for specific requirements. Interfacing with a portal will also demonstrate your ability to integrate within the enterprise, and decision makers will often sway your way when compared to a non-integrated system.

In the case of DRILS, we were able to integrate the application with the Air Force Portal that streamlined sign-on for many of our DoD users. It also allowed us to extend use of the application to selected F-16 DoD repair contractors in the .com world that facilitated increased visibility of F-16 avionics repairs worldwide.

The DRILS Air Force Portal integration went fairly smoothly with only relatively minor edits to our authentication process. We did encounter policy challenges that we felt had to be overcome. We had several hundred users who depended on the application for depot production. If the portal went offline, we risked not collecting valuable data as production would continue, but data capture may not catch up. Thus, we still wanted our users to be able to access the system. The Air Force Portal policy was that our application authentication must be restricted to portal users and deny direct access and login via our non-portal Web address. It took a few e-mails and conference calls as well as a formal waiver

request to gain approval for a hybrid security model that would allow both Air Force Portal and manual authentication. This allowed us to ensure maximum availability to at least our .mil users. Those in the .com world would have to remain dependent on the Air Force Portal availability.

Have You Done Your Paperwork?

I dislike doing paperwork as much as the next person. Unfortunately, paperwork is just part of the territory when it comes to building and fielding a DoD IT system. Recent NDAA legislation leaves you with little choice. You risk incurring stiff financial and judicial penalties if you do not complete your paperwork.

The following questions address the two main documentation areas that should be common across the DoD. Each agency may impose additional requirements. You will need to check with your respective agency for details.

Are You Registered With PfM?

PfM is your required first approval stop for any local or global data system. PfM is the management of selected groupings of investments using integrated strategic planning, integrated architectures, performance measures, risk-management techniques, transition plans, and portfolio investment strategies. The PfM process is driven by a number of legislative acts and DoD directives.

At the root of PfM is the Clinger-Cohen Act of 1996 that requires agencies to use a capital planning and investment control process to provide for selection, management, and evaluation of IT investments [8]. Consequently, the DoD published Directive 8115.01, Information Technology Portfolio Management, to establish policy and assign responsibility for the management of DoD IT investments as portfolios that focus on improving DoD capabilities and mission outcomes [9]. DoD Directive 8000.1, Management of DoD Information Resources and Information Technology, establishes the requirement for a Chief Information Officer (CIO) role in the agencies to manage these portfolios. The CIOs designate portfolio managers to manage their portfolios [10]. Portfolio managers interact with DoD IT system program managers to report the status of their programs.

The DoD Enterprise Information Technology Portfolio Repository (DITPR) is one system used to track portfolios. DITPR was selected by the DoD CIO as the enterprise shared space for IT PfM data for all DoD business IT systems. However, each branch has its own methods of IT registry that feed to DITPR. The Air Force uses the Enterprise Information Technology Data Repository (EITDR), the Navy and Marines use the DITPR-DON (Department of Navy) system, and the Army uses the Army Portfolio Management System (APMS) as their registry. All of these systems are used to record investment review and certification submission information, Federal Information Security Management Act (FISMA) of 2002 assessments, and more [11]. The IT Lean acquisition process and security, interoperability, supportability, sustainability, and usability processes are integrated into these systems as well.

These systems are necessary in order to provide portfolio managers access to information needed to do the following: maximize value of IT investments while minimizing risk, improve communication and alignment between IT and DoD leaders, facilitate team thinking versus individual commands or units, enable more efficient use of assets, reduce the number of redundant projects and eliminate non-value added projects, and support an enterprise IT investment approach.

Portfolio managers depend on IT program managers to keep the portfolio data current for their respective systems in order to fulfill their goals. Participation in PfM is not an option. There are serious consequences for not complying with all of the PfM requirements.

If you are building a new system or expanding the capability of an existing system, you must submit a capability request to your respective portfolio manager to get authorization. This is where you once again tap into your foundational data that describes the gaps you are filling. You may need to arrange a meeting with your portfolio manager to describe why you need the capability and that a similar capability does not exist. The portfolio manager has to weigh a lot of criteria when making a decision to authorize your request and may request additional data to reach their decision. You may even be invited to a *fly off* before a board who is evaluating similar systems within the portfolio.

Do You Meet the Information Assurance Requirements?

One of the first things that a portfolio manager will evaluate is whether you comply with mandatory information assurance (IA) requirements for your system. IA is more important today than it ever has been; information warfare attacks are a reality. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency [11].

In order to comply with FISMA requirements, the DoD has created the Defense Information Assurance Certification and Accreditation Process (DIACAP) that replaced the Defense Information Technology Security Certification and Accreditation Process. DIACAP assigns, implements, and validates DoDI 8500.2 standardized IA controls and manages IA posture across DoD information systems consistent with FISMA legislative policy as well as DoD regulatory policy found in the 8500 series of directives [12].

You need to ensure that your system remains compliant with the IA requirements identified in the DoD IA 8500 series of directives. If you do not, then you will not be authorized to operate on the DoD network or interface to legacy systems. DoDI 8500.2 assigns IA controls to three Mission Assurance Categories (MAC) and three data sensitivity levels. You will need to evaluate your system and select one MAC and one data sensitivity level appropriate to your system and mission that will determine what your IA control requirements are.

Once you have shown that you comply with the IA control requirements, you must submit a Certification and Accreditation (C&A) package to your Designated Approval Authority for approval using the DIACAP workflow. When your package is approved, an Authority to Operate will be issued that is valid for three years from the date it is issued. DIACAP also requires annual security reviews of the C&A package and those reviews are reported to the portfolio manager through the appropriate portfolio registry such as EITDR, DITPR-DON, or APMS.

Complying with mandatory IA requirements is just one piece of the security puzzle. You need to also ensure the system is programmed defensively using secure coding techniques to ensure that your system and its information are not compromised. Web application security is considered a weak point in an IT security wall and subject to information warfare attack.

The Defense Information Systems

Coming Events

March 3-7
SD West 2008 Software Development Conference and Expo West
Santa Clara, CA
http://sdexpo.com

March 4-5
Warfighter's Vision 2008
Tampa, FL
www.afei.org

March 11-12
2008 Military and Aerospace Electronics Forum
San Diego, CA
http://mtc08.events.pennnet.com/fl//index.cfm

March 16-18
2008 Engineering Research Council Summit, Workshop and Forum
Arlington, VA
www.asee.org/conferences/erc/2008/index.cfm.

March 17-20
2008 SEPG
Tampa, FL
www.sei.cmu.edu/sepg

March 18-20
Sea - Air - Space 2008
Washington, D.C.
www.sasexpo.org/2008

March 24-28
International Testing Certification Super Week
Chicago, IL
www.testinginstitute.com

April 29-May 2
2008 Systems and Software Technology Conference
Las Vegas, NV
www.sstc-online.org

Coming Events: Please submit coming events that are of interest to our readers at least 90 days before registration. E-mail announcements to: nicole.kentta@hill.af.mil.

Agency has published a Security Technical Implementation Guide titled "Application Security and Development Security." This can be downloaded at <http://iase.disa.mil>.

Conclusion

It is possible to grow a local product into an enterprise system with today's increased PfM and IA requirements. We started DRILS in July of 2000, delivered our rapid prototype in September of 2000, and used evolutionary development from that point forward. During my six years as chief architect, I saw a lot of transformation on how IT systems are certified and supported. I am glad to say that it is becoming less of a paperwork drill now. However, there are still a lot of steps to be checked off. You still have to do your homework and some paperwork to lay your foundation in order to educate your user community, champions, and portfolio managers on why your system should exist.

Align yourself wherever possible with the goals, objectives, and standards of your agency and the DoD in general. Pathfinders are an excellent avenue to prove your alignment, increase your visibility, and gain acceptance at the headquarters level. You can further demonstrate your capability to integrate in the enterprise by facilitating streamlined sign-on to your application through a portal such as the Air Force portal or AKO.

Getting integrated into the DoD enterprise is not only a technology challenge but also a challenge of navigating the approval process. However, with the proper preparation the approval process will be much easier to navigate successfully.◆

References

1. Lindsey, Capt. Greg, and Kevin Berk. "Serialized Maintenance Data Collection Using DRILS." CrossTalk Oct. 2003 <www.stsc.hill.af.mil/CrossTalk/2003/10/0310lindsey.pdf>.
2. Berk, Kevin. "Falcon Flex: Turning Maintenance Information into Air Power." Defense AT&L July-Aug. 2007 <www.dau.mil/pubs/dam/2007_07_08/lebr_ja07.pdf>.
3. Total Quality Systems. "UID/Falcon Flex Transforming Sustainment." Proc. of the U.S. Air Force UID/AIT Conference 2007 <www.dla.mil/j-6/AIT/Conferences/USAF_UID-AIT_Conference/default.aspx>.
4. U.S. GAO. DoD Business Systems Modernization – Billions Continue to Be Invested With Inadequate Management Oversight and Accountability. GAO-04-615. Washington: GAO, 2004.
5. Congress of the United States of America. Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005. 108th Congress, 2004 <http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4200.enr:>.
6. U.S. Air Force. "Technical Order 00-20-2, Maintenance Data Documentation." Apr. 2007.
7. Merriam Webster <www.merriamwebster.com/dictionary/ pathfinder>.
8. Congress of the United States of America. Clinger-Cohen Act of 1996. 104th Congress, 1996 <www.cio.gov/Documents/it_management_reform_act_Feb_1996.html>.
9. DoD. "DoDD 8115.01, Information Technology Portfolio Management." Oct. 2005 <www.dtic.mil/whs/directives/corres/pdf/811501p.pdf>.
10. DoD. "DoDD 8000.1, Management of DoD Information Resources and Information Technology." Feb. 2002 <www.js.pentagon.mil/whs/directives/corres/pdf/800001p.pdf>.
11. United States. "Federal Information Security Management Act (FISMA)." 2002 <www.whitehouse.gov/omb/egov/g-4-act.html>.
12. DoD. "DoDD 8500.2, Information Assurance Implementation." Feb. 2003 <www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>.

About the Author

Fred Smullin is founder and president of Integratable Technologies, LLC. He has been involved in developing software for DoD customers over the past 18 years, as well as consulting internationally on commercial software projects. Smullin served as the Chief Software Architect of the G200 DRILS from 2000 to 2006 before launching Integratable Technologies, LLC. His passion is researching how to make enterprise integration easier.

Integratable Technologies, LLC
1436 Legend Hills DR
STE 105
Clearfield, UT 84015
Phone: (801) 779-1035
Fax: (801) 779-1057
E-mail: fsmullin@integratable tech.com