

Defense Daily

December 3, 2008

Benefits of Implementing [Open Architecture](#) Reach Beyond Military's Efforts

[Full Issue](#) | [Comments](#) | [Print](#) | [Email](#) | [Archives](#) | [Copyright Permissions](#) | [RSS](#)

By Geoff Fein

While the Navy is working to incorporate [open architecture](#) (OA) into its surface ships, aviation assets and electronic systems, other federal agencies are also migrating toward the concept in hopes of increasing interoperability while at the same time demonstrating cost savings.

Those federal agencies benefit from OA in three main ways, Andy Blumenthal, Chief Technology Officer at the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), told *Defense Daily* in a recent interview.

Blumenthal added that his views on OA are his own and do not necessarily represent those of the ATF.

"First, OA helps agencies to be more interoperable. For example, by using open software standards, we can more easily consolidate disparate systems and decommission legacy systems, thereby achieving cost savings and cost avoidance," he said. "Second, OA enables agility for agencies. For example, [with] open computer architecture, we can upgrade, add, or change out components to accommodate growth, changing mission requirements, market conditions, or technologies."

OA is also critical to information sharing, Blumenthal added.

"By standardizing on open standards, we can better interoperate with other federal, state, and local agencies as well as the private sector to share information as appropriate," he said. "This is particularly important to counter-terrorism and preventing violent crime."

Although Blumenthal could not elaborate on any specific federal agency usage, he noted that while OA represents a model of efficiency and effectiveness and should be given the highest consideration, there are functional, technical or security requirements that it does not meet.

"Ultimately, this is about breaking down the culture of empire building, information hoarding, and technological puffery," he said. "Government should strive to provide the most flexible and interoperable solutions for maximum effectiveness, and customize technology only when absolutely necessary."

Aside from the technical challenges of moving toward OA systems, there are also cultural obstacles that organizations must contend with.

The first step, Blumenthal said, is to acknowledge that change is hard.

"But it becomes easier for people to stomach if they themselves are convinced of the need for change and given a role in determining how it will unfold," he said. "In an IT (information technology) context, this is accomplished through strong leadership and a robust EA (enterprise architecture) and IT governance process. The leader(s) set the vision, the EA lays a roadmap for change and the governance process is the way we actualize that change by vetting decisions with subject matter experts."

OA is an important part of the roadmap, he added. "It implements a vision of maximum governmental efficiency and effectiveness--we spend the taxpayer's money once and not twice wherever possible on open standards-based solutions."

While a few years ago it may have been difficult, if not impossible, to get different operating systems, for example, to work together. Today, though, those differences in operating systems or hardware, do not pose as serious a threat to the success of moving to OA, Blumenthal said.

"It's OK for agencies to use different hardware and software as long as they are building to common standards. I may use a Windows-based computer while you use a Macintosh, but we can still communicate over the Internet and read each other's e-mail, documents, and so forth. The key is that we are both using technologies that are built to and using common standards," he said.

As the military and federal agencies begin to implement OA, there are those who note the security risks to opening up systems. Blumenthal acknowledged that security, especially for law enforcement or military missions, cannot be compromised.

"But at the same time, it would not be feasible to have every single department, division, and office developing its own hyper-customized hardware and software," he said. "In addition, creating open standards that enable us to interoperate and share information can help make us more secure.

"One way forward is the model represented by Intellipedia in which those that are part of larger trusted community of interest (for example, the intelligence community) establish an OA within their boundaries of trust," Blumenthal added.

While risk can never be fully eliminated, it can and must be managed with balance and appropriate measures, he said.

"In the end, the migration to OA will proceed where the benefits outweigh costs, [where] leaders have articulated the vision, where people have been made ready for change, and where organization structures such as EA and governance promote OA as a strategic goal," Blumenthal said.