



CIO Issues

CIO Zalmi Azmi: Inside the FBI's I.T. Department

By Pam Baker

January 3, 2006 8:05AM

Zalmi Azmi bears the responsibility for the FBI's overall I.T. efforts, working with a budget determined three years in advance. "No one can possibly know what technology will become available -- or obsolete -- three years in the future," said Azmi. "Right now, I am working under the constraints of a budget drawn by my predecessor three years ago."

➤ No one needs to tell Zalmi Azmi what's at stake at his job. As CIO of the Federal Bureau of Investigation, he bears the responsibility for the bureau's overall I.T. efforts, including developing the strategic plan and operating budget, maintaining the technology assets, and providing technical direction for the reengineering of FBI business processes.

It is no easy task. The FBI's I.T. budget is determined three years in advance.

"No one can possibly know what technology will become available -- or obsolete -- three years in the future," said Azmi. "Right now, I am working under the constraints of a budget drawn by my predecessor three years ago."

He was appointed CIO by FBI Director Robert S. Mueller in May 2004, but the budgets Azmi developed will not go into effect until 2007. So he strives to push the existing budget to its absolute limits in making I.T. advancements in the here and now.

Prior to his appointment at the FBI, Azmi served as the CIO for the Executive Office for the United States Attorneys and as a project manager at the U.S. Patent and Trademark Office.

Azmi has a bachelor's degree in Information Systems from American University and a master's degree in Management Information Systems from George Washington University.

This ultimate keeper of secrets revealed the inside workings of the FBI's I.T. department in an interview with CIO Today. Articulate and savvy, patriotic, passionate, and pleasant, he openly shared information yet never exposed sensitive details. Here is what he had to say about the secret world of I.T. at the FBI.

CIO Today: What are your top concerns as CIO?

Azmi: Globalization is a major, major concern -- not in the commercial terms the private sector tends to think of it. Rather, in terms of national [security](#) 🇺🇸, law enforcement, and protecting national assets. There are no boundaries or borders anymore. Criminals can work from anywhere and cause harm anywhere.

A recent example: Working with law enforcement authorities in Morocco and Turkey, the FBI arrested two individuals believed to be

responsible for the creation and distribution of the Mytob and Zotob computer worms that disrupted services on computer networks of a variety of companies, including major U.S. news organizations.

The Internet is my concentration now; it is a lot of ground to protect.

CIO Today: Has the I.T. environment changed from five years ago?

Azmi: The Internet was not a household name five to 10 years ago. It is now, and it has my full attention. The private sector is mostly automated and electronic now. And the new generation of graduates is more computer-savvy, and that's changing the workplace in every field.

And, mobile technology has changed the landscape dramatically.

You know, initially agents feared that all the new technology would reduce them to the equivalent of clerks -- where they would be stuck at a desk entering data rather than out in the field looking for clues and new information. It took them a while to understand that these things are merely tools -- you can never substitute human interaction with a tool.

It is important to use the right tool to get the job done. Sometimes that means using new technology; sometimes older technology works better. It just depends on the situation.

But wireless communication is a favorite with agents since it unleashes them from their desks and helps them work in the field. Funny to think that mobile technology is really very, very new. It's hard to think of working without it now.

CIO Today: How have new legislative demands affected the I.T. department and the CIO in particular?

Azmi: Legislation demands are far more stringent and exacting on I.T. departments in government. Since we are locked into budgets designed and approved three years ago, and no one could predict new legislative requirements down the road, it really hurts us to have to

jump to fill these requirements in such an immediate and short time frame.

It is a major challenge for us to predict technology and regulatory developments three years in advance. Mostly, I am guessing what technology will be available and what it will cost in 2008 in order to develop a budget now. Trouble is, I will be estimating based on the responses of maybe four to five vendors -- but by 2008, there may be only one vendor left standing after bankruptcies and mergers and the like.

We have to do a great deal of research, not just on technological advancements, products, and services, but also on vendors and companies in order to try to predict which are likely to still be in business three years from now.

That's why we largely stay away from bleeding-edge technologies and stick with cutting-edge, because we don't have the money to risk nor the luxury of a do-over. It's impossible to make a guess at what regulations may be in place then.

CIO Today: Which enterprise component or technology will be growing most in terms of its slice of the budget pie in the next 12 months?

Azmi: The bureau has a lot of antiquated business processes. I am trying to transition the bureau to the 21st century. So, service-oriented architecture has most of our budget focus, as does business-process automation.

CIO Today: Can you walk us through the decision-making process of implementing a large-scale business process management initiative?

Azmi: We identify inefficiencies first and then define possible solutions through research and development. We also involve staff from the affected business line and a number of advisory people and boards. Majority rules and the results are included in the final budget for implementation three years down the road.

The software industry has matured, so once we define the processes needed we can often find products off the shelf to match, that require only minimal modifications. That saves money. I mean, why reinvent the wheel if you are just trying to automate time and attendance?

In other areas, more R&D and more money is needed, of course. Those projects are also budgeted for in the same way.

Robert Garrity, Deputy CIO, who was also an FBI agent for 29 years, and Jack Israel, CTO, spearhead a lot of the product-identification work.

CIO Today: What are one or two software or hardware products your company uses that you would describe as outstanding?

Azmi: I can only speak in general terms since our policy forbids brand endorsements. But I am impressed with virtualization products and data ingestion processes that convert raw data into a meaningful, searchable base.

CIO Today: Which emerging technology do you see as most important to the enterprise?

Azmi: The Enterprise Service Bus, definitely. It is the backbone of communication between all services. An end-to-end solution is vitally important.

CIO Today: Where do you go to do your research on new technologies?

Azmi: I have formed my own FBI CIO advisory council, which will be announced in the next few weeks, comprised of former CIOs and CTOs from the private and public sector that will meet as needed, but at least on a quarterly basis, as an I.T. think tank for the FBI.

I also routinely meet face to face with other CIOs to get their take on I.T. and tech developments.

My CTO works hard every day identifying tech developments and trends.

And, I have research pushed via e-mail to me on a daily basis -- some from common sources like Google, others from FBI sources.

An Inside Look at the FBI's Most-Wanted I.T. Practices

FBI CIO Zalmi Azmi faces a paradox. On the one hand, his organization has a critical need to share information with agents on the street, state and municipal law enforcement, and first responders, which calls for a degree of openness.

On the other hand, the FBI must protect the U.S. from terrorist attacks, espionage, high-tech crimes, criminal organizations, and corruption in the public and private sectors -- all of which would seem to require the FBI to keep a tight lid on its information.

The balance between securing and sharing information is a delicate one. Information sharing is crucial to safeguarding national assets and ensuring public safety, Azmi said, but, if not handled carefully, sharing can lead to vulnerability.

The FBI has developed I.T. systems that share information, be it unclassified or top secret, with law enforcement and the intelligence communities.

The FBI Intelligence Information Reports Dissemination System (FIDS) allows intelligence personnel to automate and standardize products quickly and efficiently. The FBI also has expanded its use of Law Enforcement Online (LEO) to improve information sharing with law enforcement and first responders.

The FBI is making steady progress in enterprise I.T. management and governance [infrastructure](#) 🏢. The bureau's Office of I.T. Policy and Planning (OIPP), one of four offices under Azmi, seeks to optimize I.T. resources, provide guidance for integrating I.T. strategies, and to ensure compliance with government regulations.

This year's FBI Director Team Award for Special Achievement went to OIPP for its contributions to the bureau's overall mission.

In the works is the Sentinel program, developed in conjunction with the Department of Homeland Security (DHS) and the Department of Justice (DOJ), which seeks to enhance access to information and promote information sharing. Once implemented in 2006, Sentinel will consolidate and replace the FBI's legacy case-management capabilities with an integrated, paperless file management and workflow system.

"Sentinel moves the FBI towards a flexible technology architecture," Azmi said. "Additionally, we are developing an internal cadre of trained and experienced project managers. We have defined our governance processes and have documented our Enterprise Architecture. We are now prepared to ask the commercial sector to join us in applying the best practices and enabling technology to advance FBI's mission to protect our nation from an unwanted event."

