FEATURE

# Why The G-Men Aren't I.T. Men

The FBI's new CIO must change the agency's cultural bias against information-sharing and technology before it can become a global intelligence operation truly capable of preventing crime and terrorism.

By Allan Holmes

CIO | Jun 15, 2005 8:00 AM



Robert Mueller came in as the new FBI director in September 2001, promising a fresh start. He identified upgrading FBI technology as one of his top 10 priorities. Yet two years later, not much appeared to have changed, according to several people familiar with the agency. In the summer of 2003, while Mueller and then acting CIO Wilson Lowery were interviewing Jerry Gregoire for the CIO post, Gregoire, who had been CIO for Dell Computer and Pepsi Cola, says they asked him what he would do to get VCF back on track. In response, Gregoire asked whether the FBI had considered killing VCF and starting over. The answer he recalls is, "We can't because that's not how things are done here, because you have to take the heat and go to Congress."

He adds, "I came out of that meeting saying, Holy smokes, I don't know if I can help them." Gregoire was offered and accepted the CIO job in September 2003. But within days, Lowery called him at his ranch in Austin, Texas, asking him to send a letter declining the offer, according to Gregoire. (Despite persistent requests for an explanation of why the FBI was withdrawing the offer, Gregoire did not receive any reason for the reversal.)

Gregoire was interviewed a few months after the quick departure of Darwin John, the former CIO for the Mormon Church and Scott Paper. John lasted only 10 months as FBI CIO before leaving due to what he would only describe as a disagreement on "a matter of principle" with Mueller. Looking back on his tenure as CIO, John describes the job of transforming the FBI IT operations as "the Mount Everest of IT challenges."

**A Train Wreck in Slow Motion**

That was the culture Azmi inherited in December 2003, when he left his CIO post at the U.S. Attorneys' Office to accept the acting CIO position at the FBI. (He was officially named CIO in May 2004.) When Azmi came aboard, one of the first questions he asked FBI management was how big his IT budget was. The answer Azmi received, delivered with a straight face, was $5,800. The reason: Nearly the entire FBI IT budget was controlled by field offices and other divisions in the Bureau, not the headquarters CIO. "Nothing really shocked me more," Azmi says.

Azmi also learned that the FBI had not fully complied with a law—signed by President Clinton seven years earlier—that mandated the responsibilities and competencies for federal CIOs. For instance, the FBI hadn't even developed basic IT policies, an enterprise architecture, a portfolio management strategy or a strategic plan. "I was surprised to see that an organization as large as the FBI, and with such a critical mission, [did not have in place] some of these basic things," Azmi says, shaking his head.

As for VCF, Azmi says he noticed immediately that there were too few FBI technicians compared with the number of SAIC contractors. As a result, the FBI could not keep up with communicating the ever-expanding requirements for VCF to SAIC developers. SAIC was filling in the blanks and making too many key development decisions, he says.

To meet the December 2003 deadline, SAIC created eight software teams, which included 250 full-time positions, to write software and develop applications to meet ever-evolving requirements. Turnover at the FBI caused the requirements to change frequently, both Hughes and Punaro say. Since November 2001, the FBI had 19 IT management changes. "Each change brought new directions, a different perspective on priorities and new interpretations to requirements," Punaro wrote in his testimony to Congress. In all, the FBI asked for 36 contract modifications, an average of one and a half change orders per day. The numerous requirement changes were "the most damaging aspect," Punaro testified. As a result, the price for the entire Trilogy project ballooned from an original estimate of $379.8 million in 2000 to $596 million by 2004, according to the U.S. Government Accountability Office.

In December 2003, SAIC delivered what it later described as a "snapshot in time" of the software for VCF. An independent evaluator, Aerospace Corp., tested the system as if the copy were a finished product and found numerous deficiencies. The NRC also delivered a report in May 2004 to the FBI, concluding that "the FBI's IT modernization program is not currently on a path to success." The report recommended the Bureau abandon its big-bang implementation in favor of an incremental approach and develop better program management skills and personnel.

These reports convinced the FBI that its flash cutover strategy was too ambitious. In June 2004, the agency changed its approach, requiring only that an initial operating system focusing on workflow processes be delivered by December 2004. The full operating VCF system would be delivered in 2005. SAIC delivered an initial VCF workflow process system on time, and in January, the initial VCF system was delivered to the FBI's New Orleans office for agents to test. Azmi traveled to New Orleans in March to meet with the agents and collect their reviews. He came back with bad news for Mueller. Two months after the system was deployed in New Orleans, with the FBI having spent 1,800 hours training 240 agents to use the system, Azmi reported to Mueller that the program was too complicated for agents to use.

A week later, Mueller finally informed Congress that he was going to do what IT experts say should have been done years earlier: Kill VCF.

**Airing Out the FBI**

Now a year into his job as the FBI's fifth CIO, Azmi has made some progress in building a firmer foundation for IT. In February, Mueller finally gave Azmi budget authority over the Bureau's IT budget—a rare occurrence for the federal government, in which most budget power resides with federal CFOs or with IT managers in divisions deeper down the agency's organizational chart. The budget authority will give Azmi the power to more easily consolidate IT applications and systems, and dictate standards across the agency. Azmi says he also recently solved some issues with the Bureau's enterprise architecture, and now he can consolidate systems and develop new ones based on the agency's mission to combat crime and terrorism. Azmi is close to identifying all of the FBI's IT projects to fulfill his goal of establishing a portfolio management plan. He is in the process of creating a five-year strategic plan to guide IT development and spending.

Azmi is also trying to change the agency's traditional skepticism of IT. He meets regularly with key stakeholders, such as the special agents advisory group, to solicit advice on functions for the new system to replace VCF. He also has appointed a visiting special agent (who rotates in every six months) to his staff to inform Azmi and the IT department about which technologies field agents need. In turn, the visiting agent learns how the CIO office and IT operate, information that he can take back to fellow agents. And every six months, Azmi calls an "all-hands meeting" with the entire 500-member IT staff to discuss how things are going.

In March 2005, Azmi delivered on the first promise he made when he was named CIO. The help desk typically closed at 7 p.m. EST, after which technicians were reachable only by pager. Last year, Azmi promised agents worldwide that they would have access to a round-the-clock help desk. In March, Azmi told agents that the help desk was open 24/7. I want them to know that "if they're on the job, we're on the job," Azmi says.

In late May, the FBI announced it would build a new case management system called the Sentinel in four phases. The agency is expected to issue an RFP for the project this summer. Azmi says he plans to deploy several capabilities, including workflow, document management, record management, access control, audit trails, single sign-on and PKI applications. Azmi realizes that the transition to the new system will require winning over agents first. To manage expectations, he plans to communicate often and pour lots of resources into training agents.

"We want to automate those things that are the most manually cumbersome for the agents so that they can see that technology can actually enhance their productivity," he says. "That is how to change their attitudes."

So far, Azmi has received high marks for what he has been able to accomplish. "He's made an improvement over time," says Randy Hite, the GAO's director for IT architecture and systems issues. "There are a lot of things contributing to the challenges for the organization, and some are being dealt with now."

But Congress and other government and private watchdog groups continue to cast a critical eye on the FBI's efforts to join the 21st century. In a recent report, the National Academy of Public Administration, an independent government advisory group in

Washington, D.C., raised the specter that Congress may have to pass a law requiring the FBI to develop a comprehensive information-sharing process if the Bureau does not immediately improve.

Hite says the Bureau still has a long way to climb toward elevating IT to the level in which it supports the FBI in meeting its mission of fighting crime and analyzing intelligence to fight terrorism. "It's a quantum leap from defining IT policies to making sure they are followed by the people out there managing projects," he says. "A kind way to describe the FBI is to call it a challenged organization."

Azmi is aware of the mountain that faces him—not to mention the consequences if he fails to deliver the support systems the agents need to fight against high-tech crime and terrorism. "Looking at the mission of the FBI and how critical it is, I will tell you that we are at war," he says. "And the best tool we have is information, and if information doesn't get to agents on the street in time, then we haven't done our job properly."

Allan Holmes