The Washington Post

The FBI's Upgrade That Wasn't

$170 Million Bought an Unusable Computer System

By Dan Eggen and Griff Witte
Washington Post Staff Writers
Friday, August 18, 2006

As far as Zalmai Azmi was concerned, the FBI's technological revolution was only weeks away.

It was late 2003, and a contractor, Science Applications International Corp. (SAIC), had spent months writing 730,000 lines of computer code for the Virtual Case File (VCF), a networked system for tracking criminal cases that was designed to replace the bureau's antiquated paper files and, finally, shove J. Edgar Hoover's FBI into the 21st century.

It appeared to work beautifully. Until Azmi, now the FBI's technology chief, asked about the error rate.

Software problem reports, or SPRs, numbered in the hundreds, Azmi recalled in an interview. The problems were multiplying as engineers continued to run tests. Scores of basic functions had yet to be analyzed.

"A month before delivery, you don't have SPRs," Azmi said. "You're making things pretty. . . . You're changing colors."

Within a few days, Azmi said, he warned FBI Director Robert S. Mueller III that the $170 million system was in serious trouble. A year later, it was dead. The nation's premier law enforcement and counterterrorism agency, burdened with one of the government's most archaic computer systems, would have to start from scratch.

The collapse of the attempt to remake the FBI's filing system stemmed from failures of almost every kind, including poor conception and muddled execution of the steps needed to make the system work, according to outside reviews and interviews with people involved in the project.

But the problems were not the FBI's alone. Because of an open-ended contract with few safeguards, SAIC reaped more than $100 million as the project became bigger and more complicated, even though its software never worked properly. The company continued to meet the bureau's requests, accepting payments despite clear signs that the FBI's approach to the project was badly flawed, according to people who were involved in the project or later reviewed it for the government.

Lawmakers and experts have faulted the FBI for its part in the failed project. But less attention has been paid to the role that the contractor played in contributing to the problems. A previously unreleased audit -- completed in 2005 and obtained by The Washington Post -- found that the system delivered by SAIC was so incomplete and unusable that it left the FBI with little choice but to scuttle

the effort altogether.

David Kay, a former SAIC senior vice president who did not work on the program but closely watched its development, said the company knew the FBI's plans were going awry but did not insist on changes because the bureau continued to pay the bills as the work piled up.

"SAIC was at fault because of the usual contractor reluctance to tell the customer, 'You're screwed up. You don't know what you're doing. This project is going to fail because you're not managing your side of the equation,' " said Kay, who later became the chief U.S. weapons inspector in Iraq. "There was no one to tell the government that they were asking the impossible. And they weren't going to get the impossible."

Mueller's inability to successfully implement VCF marks one of the low points of his nearly five-year tenure as FBI director, and he has accepted some of the blame. "I did not do the things I should have done to make sure that was a success," he told reporters last month.

SAIC declined three requests for comment. The company told Congress last year that it tried to warn the FBI that its "trial and error" approach to the project would not work, but it said it may not have been forceful enough with the bureau.

Whoever is at fault, five years after the Sept. 11, 2001, terrorist attacks and more than $600 million later, agents still rely largely on the paper reports and file cabinets used since federal agents began chasing gangsters in the 1920s.

1980s Technology

Even before the Sept. 11 attacks, the FBI had developed a plan, Trilogy, to address its chronic technology problems. The program was made up of three main components: a new computer network, thousands of new personal computer stations and, at its heart, the software system that would come to be known as VCF.

The FBI wanted its agents to work in a largely paperless environment, able to search files, pull up photos and scan for information at their own PCs. The old system was based on fusty mainframe technology, with a text-only "green screen" that had to be searched by keywords and could not store or display graphics, photos or scanned copies of reports.

What's more, most employees had no PCs. They relied instead on shared computers for access to the Internet and e-mail. A type of memo called an electronic communication had to be printed out on paper and signed by a supervisor before it was sent. Uploading a single document took 12 steps.

The setup was so cumbersome that many agents stopped using it, preferring to rely on paper and secretaries. Technologically, the FBI was trapped in the 1980s, if not earlier.

"Getting information into or out of the system is a challenge," said Greg Gandolfo, who spent most of his 18-year FBI career investigating financial crimes and public corruption cases in Chicago, Little Rock and Los Angeles. "It's not like 'Here it is, click' and it's in there. It takes a whole series of steps and screens to go through."

Gandolfo, who now heads a unit at FBI headquarters that fields computer complaints, said the biggest drawback is the amount of time it takes to handle paperwork and input data. "From the case agent's point of view, you want to be freed up to do the casework, to do the investigations, to do the intelligence," he said.

At the start, the software project had relatively modest goals -- and much lower costs. When SAIC beat out four competitors to win the contract in June 2001, the company said it would be earning $14 million in the first year of a three-year deal to update the FBI's case-management system.

For SAIC, the contract was relatively minor. The firm, owned by 40,000 employee shareholders, is one of the nation's largest government contractors. The 2001 attacks were a boon to its fortunes, helping to boost its annual revenue, now more than $7 billion.

At the FBI, the impact of the attacks was equally significant but certainly less auspicious. As revelations emerged that the bureau had missed clues that could have revealed the plot, its image suffered. Its long-outdated information technology systems drew particular scrutiny.

"Prior to 9/11, the FBI did not have an adequate ability to know what it knew," a report by the staff of the Sept. 11 commission concluded. "The FBI's primary information management system, designed using 1980s technology already obsolete when installed in 1995, limited the Bureau's ability to share its information internally and externally."

The problems continued to hamper the bureau after the attacks as well: To transmit photographs of the 19 Sept. 11 hijackers and other suspects to field offices, headquarters had to fax copies or send compact discs by mail, because the system would not allow them to e-mail a photo securely.

In the months after the terrorist attacks, overhauling the case-management system became one of the bureau's top priorities. Deadlines were moved up, requirements grew, and costs ballooned.

Along the way, the FBI made a fateful choice: It wanted SAIC to build the new software system from scratch rather than modifying commercially available, off-the-shelf software. Later, the company would say the FBI made that decision independently; FBI officials countered that SAIC pushed them into it.

More than two years after Sept. 11, when a team of researchers from the National Research Council showed up to review the status of Trilogy, FBI officials assured them that the bureau had made great strides. That was true in part: By early 2004, two of the three main pillars of the program -- thousands of new PCs and an integrated hardware network -- were well on the way to being delivered and installed.

But, as the researchers soon learned, the heart of the makeover, VCF, remained badly off track. In its final report, in May 2004, the NRC team warned that the program was "currently not on a path to success."

The review team from the NRC, which is affiliated with the National Academy of Sciences, was made up of more than a dozen scientists and engineers from top universities and leading technology companies, all of them independent of the FBI and its contractors.

The report observed that the rollout of the new case-management software had been poorly planned nearly from the beginning. Months after the program was supposed to be complete, it remained riddled with shortcomings:

· Agents would not be able to take copies of their cases into the field for reference.

· The program lacked common features, such as bookmarking or histories, that would help agents navigate through millions of files.

· The system could not properly sort data.

· Most important, the FBI planned to launch the new software all at once, with minimal testing beforehand. Doing so, the NRC team concluded, could cause "mission-disruptive failures" if the software did not work, because the FBI had no backup plan.

"That was a little bit horrifying," said Matt Blaze, a professor of computer science at the University of Pennsylvania and a member of the review team. "A bunch of us were planning on committing a crime spree the day they switched over. If the new system didn't work, it would have just put the FBI out of business."

The NRC team found plenty of blame to go around, starting with the FBI itself.

Like many government agencies, the bureau had been drained of much of its top talent as skilled managers left for the higher salaries and reduced bureaucracy of the private sector. By 2001, when the VCF program was born, the FBI had few people in house with the expertise to develop the kind of sophisticated information technology systems that it would need. As a result, the agency had been turning increasingly to private contractors for help, a process that only hastened the flow of talent out the door at FBI headquarters.

"In essence, the FBI has left the task of defining and identifying its essential operational processes and its IT concept of operations to outsiders," the NRC researchers concluded. "The FBI lacks experienced IT program managers and contract managers, which has made it unable to deal aggressively or effectively with its contractors."

Daniel Guttman, a fellow at Johns Hopkins University who specializes in government contracting law, said: "This case just shows the government doesn't have a clue. Yet the legal fiction is that the government knows what it's doing and is capable of taking charge. The contractors are taking advantage of that legal fiction."

In the end, the FBI's failure to police the contractors would lead to disastrous results.

After the disappointing preview of VCF in late 2003 by Azmi, who was then an adviser to Mueller tasked with reviewing the system, the FBI scrambled to rescue the project. The Aerospace Corp., a federally funded research-and-development firm in El Segundo, Calif., was hired for $2 million in June 2004 to review the program and come up with a "corrective action plan."

The conclusion: SAIC had so badly bungled the project that it should be abandoned.

In a 318-page report, completed in January 2005 and obtained by The Post under the Freedom of Information Act, Aerospace said the SAIC software was incomplete, inadequate and so poorly designed that it would be essentially unusable under real-world conditions. Even in rudimentary tests, the system did not comply with basic requirements, the report said. It did not include network-management or archiving systems -- a failing that would put crucial law enforcement and national security data at risk, according to the report.

"From the documents that define the system at the highest level, down through the software design and into the source code itself, Aerospace discovered evidence of incompleteness, lack of follow-through, failure to optimize and missing documentation," the report said.

Others joined Aerospace in highlighting SAIC's role in the failure. The NRC report complains that the contractor dealt with Trilogy as a "business as usual" program, without regard to its importance to national security.

Matthew Patton, a programmer who worked on the contract for SAIC, said the company seemed to make no attempts to control costs. It kept 200 programmers on staff doing "make work," he said, when a couple of dozen would have been enough. The company's attitude was that "it's other people's money, so they'll burn it every which way they want to," he said.

Patton, a specialist in IT security, became nervous at one point that the project did not have sufficient safeguards. But he said his bosses had little interest. "Would the product actually work? Would it help agents do their jobs? I don't think anyone on the SAIC side cared about that," said Patton, who was removed from the project after three months when he posted his concerns online.

Azmi said that "in terms of having a lot of money, we were just coming out of 9/11, and at that time there was a lot of pressure on the FBI to develop capabilities for storing information and actually, for lack of better words, connecting the dots. If SAIC took advantage of that, I would say shame on them."

Mueller has also criticized SAIC, telling Congress that the software it produced "was not what it should be in order to make it the effective tool for the FBI, and it requires us now to go a different route."

One FBI manager estimated that the scope of the Trilogy project as a whole expanded by 80 percent since it began, according to a February 2005 report by Justice Department Inspector General Glenn A. Fine.

SAIC has consistently said that it was trying to meet the FBI's needs but that its efforts were undermined by the bureau's chronic indecision. Executive Vice President Arnold Punaro submitted testimony to Congress in February 2005 citing 19 government personnel changes in three years that kept the program's direction in flux.

FBI officials, he said, took a "trial and error, 'we will know it when we see it' approach to development." Punaro said the company warned bureau officials that such a method would not work, but he acknowledged that SAIC did not do enough to get the FBI's attention.

"We clearly failed to get the cumulative effect of these changes across to the FBI consumer," he said.

Punaro also faulted Aerospace, saying that its study was based on an earlier version of VCF software and that the firm "did not bring a sufficient understanding of the uniqueness, complexity and scope of the FBI undertaking to evaluate our product."

Starting Over, Again

By 2004, even as the news grew worse behind the scenes, FBI officials struggled to put an optimistic spin on their software upgrade.

In March, testifying before a House subcommittee, Mueller said that the FBI had experienced "a delay with the contractor" but that the problem had been "righted." He said he expected that "the last piece of Virtual Case File would be in by this summer."

Two months later, Azmi -- who had been named the bureau's chief information officer -- pushed back the estimate further, predicting that SAIC would deliver the product in December.

But the problems continued to mount. The FBI and SAIC feuded over change orders, system requirements and other issues, according to an investigative report later prepared for the House Appropriations Committee. The FBI also went ahead with a $17 million testing program for the system, one of many missed opportunities to cut its losses, according to the House report.

Azmi defends the attempt to save VCF and calls the decision to abandon it in early 2005 "probably the toughest" of his career.

The decision to kill VCF meant that the FBI's 30,000-plus employees, including more than 12,000 special agents, had to continue to rely on an "obsolete" information system that put them at "a severe disadvantage in performing their duties," according to the report by Fine, of the Justice Department.

"The urgent need within the FBI to create, organize, share and analyze investigative leads and case files on an ongoing basis remains unmet," Fine's office concluded.

Maureen Baginski, the FBI's former executive assistant director of intelligence, said the lack of a modern case-management system could hurt the bureau when time is of the essence. Agents and analysts need the new system, she said, to quickly make connections across cases -- especially when they are tackling complex challenges such as unraveling a terrorist plot.

Last year, FBI officials announced a replacement for VCF, named Sentinel, that is projected to cost $425 million and will not be fully operational until 2009. A temporary overlay version of the software, however, is planned for launch next year.

The project's main contractor, Lockheed Martin Corp., will be paid $305 million and will be required to meet benchmarks as the project proceeds. FBI officials say Sentinel has survived three review sessions and is on budget and on schedule.

SAIC is not involved. FBI officials say they are awaiting an audit by a federal contracting agency before deciding whether to attempt to recoup costs from the company.

In a follow-up to its reviews, Fine's office warned in March that the FBI is at risk of repeating its mistakes with Sentinel because of management turnover and weak financial controls. But Azmi and other FBI officials say Sentinel is designed to be everything VCF was not, with specific requirements, regular milestones and aggressive oversight.

Randolph Hite, who is reviewing the program for the Government Accountability Office, said: "When you do a program like this, you need to apply a level of rigor and discipline that's very high. That wasn't inherent in VCF. My sense is that it is inherent in Sentinel."

But no one really knows how much longer the bureau can afford to wait.

"We had information that could have stopped 9/11," said Sen. Patrick J. Leahy (Vt.), the ranking Democrat on the Senate Judiciary Committee. "It was sitting there and was not acted upon. . . . I haven't seen them correct the problems. . . . We might be in the 22nd century before we get the 21st-century technology."

View all comments **that have been posted about this article.**