Who Killed the Virtual Case File?

By: **Harry Goldstein**

In the early 1990s, Russian mobsters partnered with Italian Mafia families in Newark, N.J., to skim millions of dollars in federal and New Jersey state gasoline and diesel taxes. Special Agent Larry Depew set up an undercover sting operation under the direction of Robert J. Chiaradio, a supervisor at the Federal Bureau of Investigation's Washington, D.C., headquarters.

Depew collected reams of evidence from wiretaps, interviews, and financial transactions over the course of two and a half years. Unfortunately, the FBI couldn't provide him with a database program that would help organize the information, so Depew wrote one himself. He used it to trace relationships between telephone calls, meetings, surveillance, and interviews, but he could not import information from other investigations that might shed light on his own. So it wasn't until Depew mentioned the name of a suspect to a colleague that he obtained a briefcase that his friend had been holding since 1989.

"When I opened it up, it was a treasure trove of information about who's involved in the conspiracy, including the Gambino family, the Genovese family, and the Russian components. It listed percentages of who got what, when people were supposed to pay, the number of gallons. It became a central piece of evidence," Depew recalled during an interview at the FBI's New Jersey Regional Computer Forensic Laboratory, in Hamilton, where he is the director. "Had I not just picked up the phone and called that agent, I never would have gotten it."

A decade later, Depew's need to share information combined with his do-it-yourself database skills and connection to his old supervisor, Chiaradio, would land him a job managing his first IT project–the FBI's Virtual Case File.

Depew's appointment to the FBI's VCF team was an auspicious start to what would become the most highly publicized software failure in history. The VCF was supposed to automate the FBI's paper-based work environment, allow agents and intelligence analysts to share vital investigative information, and replace the obsolete Automated Case Support (ACS) system. Instead, the FBI claims, the VCF's contractor, Science Applications International Corp. (SAIC), in San Diego, delivered 700 000 lines of code so bug-ridden and functionally off target that this past April, the bureau had to scrap the US $170 million project, including $105 million worth of unusable code. However, various government and independent reports show that the FBI—lacking IT management and technical expertise—shares the blame for the project's failure.

In a devastating 81-page audit, released in 2005, Glenn A. Fine, the U.S. Department of Justice's inspector general, described eight factors that contributed to the VCF's failure. Among them: poorly defined and slowly evolving design requirements; overly ambitious schedules; and the lack of a plan to guide hardware purchases, network deployments, and software development for the bureau.

Fine concluded that four years after terrorists crashed jetliners into the World Trade Center and the Pentagon, the FBI, which had been criticized for not "connecting the dots" in time to prevent the attacks, still did not have the software necessary to connect any new dots that might come along. And won't for years to come.

"The archaic Automated Case Support system—which some agents have avoided using—is cumbersome, inefficient, and limited in its capabilities, and does not manage, link, research, analyze, and share information as effectively or timely as needed," Fine wrote. "[T]he continued delays in developing the VCF affect the FBI's ability to carry out its critical missions."

This past May, a month after it officially ended the VCF project, the FBI announced that it would buy off-the-shelf software at an undisclosed cost to be deployed in phases over the next four years. Until those systems are up and running, however, the FBI will rely on essentially the same combination of paper records and antiquated software that the failed VCF project was supposed to replace. The only recent addition has been a new "investigative data warehouse" that combines several of the FBI's crime and evidence databases into one. It was completed as the VCF started its final slide into oblivion. In addition, the FBI recently digitized millions of its paper documents and made them available to agents.

As the FBI gears up to spend hundreds of millions more on software over the next several years, questions persist as to how exactly the VCF went so terribly wrong and whether a debacle of even bigger proportions looms on the horizon. Despite high-profile Congressional hearings, hundreds of pages of reports churned out by oversight bodies, and countless anguished articles in the trade press and mainstream media, the inner workings of the project and the major players have remained largely invisible. Now, detailed interviews with people directly involved with the VCF paint a picture of an enterprise IT project that fell into the most basic traps of software development, from poor planning to bad communication.

Lost amid the recriminations was an early warning from one member of the development

team that questioned the FBI's technical expertise, SAIC's management practices, and the competence of both organizations. Matthew Patton, a security expert working for SAIC, aired his objections to his supervisor in the fall of 2002. He then posted his concerns to a Web discussion board just before SAIC and the FBI agreed on a deeply flawed 800-page set of system requirements that doomed the project before a line of code was written. His reward: a visit from two FBI agents concerned that he had disclosed national security secrets on the Internet.

To understand why the VCF was so important, you've got to understand the FBI. And to understand the FBI, you've got to understand its organization and its agents. The bureau, headquartered in the J. Edgar Hoover Building in Washington, D. C., currently has 23 divisions, including counterintelligence, criminal investigation, and cybercrime. The divisions fall under the control of five executive assistant directors responsible for intelligence, counterterrorism and counterintelligence, criminal investigations, law enforcement services (such as labs and training), and administration. Until last year, each division had its own IT budget and systems. And because divisions had the freedom and money to develop their own software, the FBI now has 40 to 50 different investigative databases and applications, many duplicating the functions and information found in others. Last year, in an effort to centralize IT operations and eliminate needless redundancies, the FBI's chief information officer, who reports to the director, took charge of all its IT budgets and systems.

The bureau's 12 400 agents work out of 56 field offices and 400 satellite—or resident agency—offices, as well as 51 Legal Attach offices scattered across the globe in U.S. embassies and consulates. A field agent works as part of a squad; each squad has a supervisor, who reports to the assistant special agent in charge, who in turn reports to the special agent in charge of the field office. Agents investigate everything from counterterrorism leads to bankruptcy fraud, online child pornography rings to corrupt public officials, art thefts to kidnappings. They interview witnesses, develop informants, conduct surveillance, hunt for clues, and collaborate with local law enforcement to find and arrest criminals. Agents document every step and methodically build case files. They spend a tremendous amount of time processing paperwork, faxing and FedEx-ing standardized memo and requisition forms through the approval chain—up to the squad supervisor and eventually to the special agent in charge. This system of forms and approvals stretches back to the 1920s, when J. Edgar Hoover, director from 1924 to 1972, standardized all of the bureau's investigative reports on forms, so an agent could walk into any FBI office and find the same system.

Today, the bureau has hundreds of standard forms. To record contact with an informant, fill out Form FD-209. When getting married or divorced, complete Form FD-292. To report information gleaned from an interview that may later become testimony, use Form FD-302. To conduct a wiretap, file Form FD-472. To wire an informant with a body recorder and transmitter, submit Form FD-473. After traveling overseas for business or pleasure, report the experience on Form FD-772. Plan an arrest with Form FD-888. Open a drug investigation with Form FD-920.

Forms related to investigations, such as those used to report interviews with witnesses, wend their way up and down the approval chain. Once the appropriate supervisors sign off on the form, it goes back to the agent, who gives it to a clerk to enter into the ACS system. From there, the paper form is filed as part of the official record of the case.

Sometimes, though the FBI officially denies this, an agent doesn't enter all case notes into ACS. Some agents think, "If I don't trust ACS because I don't think it will protect my informant or my asset, I'm not putting the data in there," said Depew, an avid user of ACS who touted the electronic system to his fellow agents as safer than a paper filing system.

FBI spokesperson Megan Baroska emphasized in an e-mail that Depew did not speak for the bureau in this instance. "The FBI policy is for all official records to be entered into ACS. Additionally, 'notes' per say [sic] are not entered into ACS; they are first memorialized in a 302 form, and that form is entered into ACS. As for the 'notes,' they are kept in storage as a paper file because they legally have to be discoverable."

When asked during an interview at FBI headquarters if agents felt uncomfortable about exchanging a paper-based system for an electronic one, the FBI's current CIO, Zalmai Azmi, didn't think agents would find it hard to get into the habit of processing forms electronically. But introducing an electronic record-keeping system does raise legal policy questions in their minds. "What is a record and what is available under discovery? In a paper world, you do your job, you do your notes, and if you don't like it, it goes somewhere," Azmi said. "In an electronic world, nothing really is destroyed; it's always somewhere."

Despite agents reluctance to embrace the digital age, in 2000 the bureau finally began to deal with its outdated IT systems. At the time, under the direction of Louis J. Freeh, the bureau had neither a CIO nor documentation detailing its IT systems, much less a plan for revamping them. The task of creating such a plan fell to former IBM executive Bob E. Dies, who became assistant director in charge of the FBI Information Resources Division on 17 July 2000. He was the first of five officials who, over the next four years, would struggle to lead the FBI's sprawling and antiquated information systems and get the VCF project under way.

According to a 2002 report from the DOJ's Office of the Inspector General, when Dies arrived, 13 000 computers could not run modern software. Most of the 400 resident agency offices were connected to the FBI intranet with links about the speed of a 56-kilobit-per-second modem. Many of the bureau's network components were no longer manufactured or supported. And agents couldn't e-mail U.S. Attorney offices, federal agencies, local law enforcement, or each other; instead, they typically faxed case-related information.

In September 2000, Congress approved $379.8 million over three years for what was then called the FBI Information Technology Upgrade Project. Eventually divided into three parts, the program became known as Trilogy. The Information Presentation Component would provide all 56 FBI field offices, some 22 000 agents and support staff, with new Dell Pentium PCs running Microsoft Office, as well as new scanners, printers, and servers. The Transportation Network Component would provide secure local area and wide area networks, allowing agents to share information with their supervisors and each other.

But the User Applications Component, which would ultimately become the VCF, staked out the most ambitious goals. First, it was to make the five most heavily used investigative applications—the Automated Case Support system, IntelPlus, the Criminal Law Enforcement Application, the Integrated Intelligence Information Application, and the Telephone Application—accessible via a point-and-click Web interface. Next, it would rebuild the FBI's intranet. Finally, it was supposed to identify a way to replace the FBI's 40-odd investigative software applications, including ACS.

Based on the 1970s-era database Adabas and written in a programming language called Natural, both from Software AG, Darmstadt, Germany, the Automated Case Support system, which debuted in 1995, was antiquated even as it was deployed—and it is still being used today. Originally, agents and clerks accessed the program via vintage IBM 3270 green-screen terminals connected to a mainframe over dedicated lines. Eventually, the 3270 terminals were emulated on standard desktop PCs. By navigating complicated menus using function keys and keystroke commands, agents could do basic Boolean and keyword searches for things like an informant's name or the dates of a wiretap surveillance, information related to cases they were working. But according to Depew, only the most dedicated, computer-savvy agents had the skills and patience to learn the arcane system, let alone exploit it to its full potential.

"Nobody really understood why we would even use ACS other than as an index," said Depew. A notable exception: Robert Hanssen, the notorious FBI traitor, used the system to find documents his Russian handlers might find useful, as well as to check to see if anyone at the FBI was onto him [see "Mission Impossible," IEEE Spectrum, April 2003].

In May and June 2001, the bureau awarded Trilogy contracts to two major U.S. government contractors: DynCorp, of Reston, Va., for the hardware and network projects, and to SAIC for software. All three Trilogy components were to be delivered by the middle of 2004. Instead of paying a fixed price for the hardware, networks, and software, the FBI used cost-plus-award fee contracts. These would pay the cost of all labor and materials plus additional money if the contractor managed costs commendably. Crucially, if the scope of the project expanded or if the contractor incurred other unforeseen costs, the FBI would have to pick up those, too.

On 4 September 2001, Robert S. Mueller III became the tenth director in FBI history. One week later, terrorists pulverized New York City's World Trade Center and a piece of the Pentagon. The inability of FBI agents to share the most basic information about Al Qaeda's U.S. activities blew up into a front-page scandal. Within days, the FBI's pathetic technology infrastructure went from being so much arcane trivia to a subject of daily fulmination by politicians and newspaper columnists. As The 9/11 Commission Report would conclude in 2004, "the FBI's information systems were woefully inadequate. The FBI lacked the ability to know what it knew; there was no effective mechanism for capturing or sharing its institutional knowledge."

In the face of intense public and congressional pressure, Mueller shifted Trilogy into high gear. In October, he pulled Chiaradio up from his position as special agent in charge of the field office in Tampa, Fla., to Hoover Building headquarters in Washington, to advise him on the all-important software component of Trilogy. An accountant by training, Chiaradio would become the FBI's executive assistant director for administration in December 2001.

After discussions with Mueller, Chiaradio determined that the FBI's basic plan for the software portion of Trilogy—slapping a Web interface onto the ACS system and the four other programs—wasn't going to make agents more effective. So to help him figure out what would work, he brought in Depew. [See timeline, "Countdown to Catastrophe."]

Partial to dark suits and wraparound shades, Depew kept his gray hair closely cropped and a pistol holstered on his belt. He was a G-man's G-man. And he embraced technology with an almost evangelical zeal. When he was working the New Jersey fuel oil case in the early 1990s, Depew not only coded his own case management database using the FoxPro program, but he put it on floppy disks and gave it to any agent who asked for a copy.

Depew joined a team of seven that assessed the Web interface SAIC was designing for the ACS system. When completed, the interface would let agents point and click their way through the tedious process of filling out official forms, but not much else. Recognizing the limitations of the interface and ACS, Chiaradio and Depew met with Dies. They

convinced him, and later the director himself, that the bureau needed an entirely new database, graphical user interface, and applications, which would let agents search across various investigations to find relationships to their own cases. The new case management system would host millions of records containing information on everything from witnesses, suspects, and informants to evidence such as documents, photos, and audio recordings. To address concerns being raised by intelligence experts and lawmakers in the wake of 9/11, these records would be accessible to both the FBI's agents and its intelligence analysts. Chiaradio dubbed the new system the Virtual Case File.

Dies wanted to provide agents with this software as fast as possible. In Depew's view that meant "shooting from the hip." This cavalier approach to software development would prove fatal to the VCF. Today, many organizations rely on a blueprint—known in IT parlance as an enterprise architecture—to guide hardware and software investment decisions. This blueprint describes at a high level an organization's mission and operations, how it organizes and uses technology to accomplish its tasks, and how the IT system is structured and designed to achieve those objectives. Besides describing how an organization operates currently, the enterprise architecture also states how it wants to operate in the future, and includes a road map—a transition plan—for getting there.

The problem was, the FBI didn't have such a blueprint, as numerous reports from the Government Accountability Office, the DOJ's inspector general, and the National Research Council subsequently pointed out. Without it, the bureau could not, as a 2004 report from the NRC stated, "make coherent or consistent operational or technical decisions" about linking databases, creating policies and methods for sharing data, and making tradeoffs between information access and security.

With no detailed description of the FBI's processes and IT infrastructure as a guideline, Depew said that his team of agents began "to feel our way in the dark," to characterize investigative processes such as witness interviews and surveillance operations and map them to the FBI's software and databases. Over a six-week period in the fall of 2001, Depew's group defined how agents worked, how they gathered information, and how that information was fed into ACS. Working with engineers from SAIC, they drew up diagrams and flowcharts of how the case management system operated then and how they wanted the new case management system, the VCF, to operate in the future. Mueller himself attended one of these meetings to tell the agents to design a system that would work best for them and not to feel constrained by 50-year-old business rules.

Depew's team also called in people from across the FBI: a dozen in the first few weeks; 40 by the end of November. These "subject matter experts" explained how their divisions or units functioned internally and with the rest of the bureau.

In December 2001, the FBI asked SAIC to stop building a Web front end for the old programs. (Later, FBI computer specialists would create a Web interface as a stopgap, which is still used by agents today, until the VCF was delivered.) Instead, SAIC was asked to devise a new application, database, and graphical user interface to completely replace ACS.

To formally define what users needed the VCF to do for them, SAIC embarked on a series of Joint Application Development (JAD) sessions. In these meetings, Depew's team of agents and experts got together with a group of SAIC engineers to hash out what functions the VCF would perform. Ideas captured in these sessions formed the basis of the requirements document that guided SAIC's application designers and programmers.

In January 2002, the FBI requested an additional $70 million to accelerate Trilogy; Congress went further, approving $78 million. DynCorp committed to delivering its two components by July 2002. SAIC agreed to deliver the initial version of the VCF in December 2003 instead of June 2004.

SAIC and the FBI were now committed to creating an entirely new case management system in 22 months, which would replace ACS in one fell swoop, using a risky maneuver known in the IT business as a flash cutover. Basically, people would log off from ACS on Friday afternoon and log on to the new system on Monday morning. Once the cutover happened, there was no going back, even if it turned out that the VCF didn't work. And there was no plan B.

But while the Trilogy contracts were changed to reflect the aggressive new deadlines, neither the original software contract nor the modified one specified any formal criteria for the FBI to use to accept or reject the finished VCF software, as the Inspector General reported earlier this year. Furthermore, those contracts specified no formal project schedules at all, let alone milestones that SAIC and DynCorp were contractually obligated to meet on the way to final delivery.

In reaction to the new deadline, SAIC broke its VCF development group into eight teams, working in parallel on different functional pieces of the program, in order to finish the job faster. But the eight threads would later prove too difficult for SAIC to combine into a single system. Nevertheless, in an interview at SAIC's McLean, Va., office complex, Rick Reynolds, vice president and operations manager for SAIC, defended the decision to change tactics. "People forget the urgency that we were underand our customer was under. And we were right beside them," he declared. "Wewere in the foxhole together."

At Hoover Building headquarters, Depew's team was hard at work describing the FBI's investigative and administrative processes: how agents built case files, how case files were

used, and what additional functions they wanted the Virtual Case File to perform. While Depew and his team prepared to communicate the processes that define the FBI to SAIC engineers, Mueller, Dies, and Chiaradio recruited a seasoned IT program manager.

Before coming to the FBI, C.Z. ("Sherry") Higgins, a 29-year veteran of AT&T and Lucent, was running the help desk at the Technology Command and Control Center for the 2002 Winter Olympics in Salt Lake City. As project management executive for the Office of the Director, Higgins was brought in to create the Office of Program Management. Higgins's new office would centralize IT management and oversee, develop, and deploy the bureau's most expensive, complex, and risky projects. But her most important assignment was to manage Trilogy.

Higgins, who left the FBI in June 2004, lives in a Cape Codstyle house overlooking a pond deep in the exurbs of Atlanta, in her native Georgia. During an interview in her living room, three fat scrapbooks of her two and a half years at the FBI peeked out from beneath a coffee table covered with candles. Her first move when she came on board in March 2002, she explained, was to appoint Depew, who had no IT project management experience, the VCF project manager.

"I'm totally accountable for that," she acknowledged. "We talked a long time about could he play the role of project manager and still be customer advocate. And we felt like he could."

Higgins and Depew had developed a rapport quickly. Just a couple of weeks after she started work at FBI headquarters, Depew invited her to the Thursday "board meeting"—pizza and beer with his team at a neighborhood joint. As the group started walking to the restaurant, Higgins, surrounded by agents in dark suits and sunglasses, asked them to stop so she could savor the moment. "I have arrived," she announced. "I'm on Pennsylvania Avenue with men in black!"

The men in black had been specifying the VCF's requirements with SAIC engineers for several weeks when Higgins shifted Depew into the driver's seat. By this point, Depew, the former Trenton, N.J.based bureau man, had rented an apartment in Washington, where he would live, separated from his family, for the next three years. He was responsible for a team of seven agents, each of whom acted as an advocate for a group of subject matter experts in the periodic JAD meetings with SAIC engineers that the team was attending.

"People forget the urgency that we were under and our customer was under," said SAIC's Reynolds. "And we were right beside them. We were in the foxhole together."

Over a six-month period, the JAD team met in two-week sessions, laying the unstable foundation for the VCF. Every day of each session, engineers from SAIC would sit with the agents and experts to chart existing and future processes on whiteboards. According to Higgins, sometimes agents would propose Web-page designs for particular portions of the user interface. So that the crowded meetings would stay orderly, people were assigned speaker and observer cards. Depew acted as a facilitator, running the meetings and telling people whether something they wanted was or was not within the scope of the project.

"There were times when SAIC and I disagreed on what's in the scope," Depew recalled. Sometimes they would agree to "push that off to other people to decide whether that's in the scope of the current contract."

After a two-week JAD session finished, a two-week feedback cycle would begin. SAIC provided Depew's team with information gleaned from the session, including needs statements, flow charts, and meeting minutes. Depew's team reviewed these materials and gave SAIC feedback while simultaneously preparing subject matter experts for the next round of JAD sessions, which immediately followed the feedback cycle. There were no breaks.

"I worked seven days a week, 14 hours a day," Depew recalled. "Six months of JAD was hell."

Meanwhile, Higgins was finding it rough going herself. She asked her colleagues at the FBI and managers at DynCorp, which was working on the hardware (computers and network) portions of Trilogy, for copies of the two project schedules. She was told the delivery dates instead. In contrast, SAIC, with its programmers pecking away at its secure data center in Vienna, Va., always had a detailed schedule posted prominently in the "war room" there, which Higgins's team would review with SAIC periodically, she said.

In mid-April 2002, Higgins gave DynCorp a week to deliver a detailed schedule. After she got it, she pulled the project teams from the FBI and DynCorp into a meeting and went through the document. Shortly after that, Higgins broke the news to the director: the computers and networks would not be delivered in July of that year as had been scheduled. She told Mueller that DynCorp didn't stand a chance of hitting the delivery target, because it didn't have a detailed schedule that mapped out how it would deploy,

integrate, and test the new computers and networks.

Mueller blamed himself for the delay, because he'd asked for an accelerated schedule. But Higgins blamed Mueller's staff for not being straight with him about his agency's ability to deliver what he wanted.

"Did somebody come to you and say, okay, Mr. Director, sir, you can have it sooner, but it's going to cost you this much more money or you're going to have to do without something?" Higgins remembered asking Mueller. "And he said, 'No, nobody ever told me that.' And I said, 'Well, lesson No. 1: faster, cheaper, better. Pick two, but you can't have all three.'"

With costs escalating and schedules slipping, Mueller had just one choice left: better. And he didn't even get that with the VCF.

But in the summer of 2002, it certainly seemed as if the Virtual Case File would be a vast improvement over the Automated Case Support system. The JAD sessions had produced an exhaustively detailed requirements document. This plan for a case-management system would combine the ACS with two other systems: the Telephone Application, the bureau's central repository of telephone records related to investigations, and parts of the Criminal Law Enforcement Application, a repository for investigative data about people, organizations, locations, vehicles, and communications.

The VCF system would accept scanned documents, photographs, and other electronic media—to simplify evidence tracking. People with the proper credentials would be able to access that evidence from any FBI office. The way work flowed through the bureau would change dramatically, too. Instead of filling out a form either by hand or in a word-processing program and then faxing or FedEx-ing the paper form to a supervisor, an agent would fill out a form online and, with a click of the mouse, route it to the supervisor. The document would pop up in a supervisor's in-box, and the agent could track it to see if it had been approved. And perhaps most important, information collected within a case file would eventually be available to software applications that would compare data among cases to search for correlations—to connect the proverbial dots.

In a Senate hearing in July 2002, Higgins impressed lawmakers, including Senator Charles E. Schumer (D-N.Y.)—"That Southern charm gets me every time," an apparently smitten Schumer gushed—with a PowerPoint presentation about the VCF. Higgins contrasted the 12 different screens agents had to navigate to upload one form into ACS with the single screen they would use to perform a similar task in the new system. Higgins told the senators that the initial version of a user-friendly, secure system would be delivered by December 2003. The senators seemed satisfied that the VCF would address their gravest concerns about the FBI's IT systems by giving agents and intelligence analysts the ability to correlate and share the data needed to prevent future terrorist attacks. Higgins had reassured the senators—and scored some choice memorabilia: a Senate coaster and her nameplate for her scrapbook.

In the Summer of 2002, turmoil roiled the FBI's IT management. In May, Bob Dies, the CIO who had launched Trilogy, left the bureau, turning over his duties to Mark Tanner, who held the position of acting CIO for just three months, until July 2002. He stepped aside for Darwin John, former CIO for the Mormon Church. Chiaradio, who declined to be interviewed for this article, left for a lucrative job in the private sector with BearingPoint Inc., a global consultancy in McLean, Va., and was replaced by W. Wilson Lowery Jr. Within a year, Lowery would replace John.

At the same time, SAIC was staffing up. By August 2002, it had around 200 programmers on the job. It was still looking for help, particularly for its security team, which was reviewing design documents that described the VCF software's overall structure, algorithms, and user interface, along with the ways data would be defined and handled.

Matthew Patton answered an ad on SAIC's Web site for security engineers. A 1995 Carnegie Mellon University graduate with a B.S. in information and decision systems, Patton had financed college through service as a cadet in the U.S. Air Force Reserve Officers' Training Corps. After college, he spent his four-year tour of military duty at the Pentagon in the Office of the Secretary of Defense. There he designed and helped program the database and security components for a Web-based application used to plan the Department of Defense's $400 billion budget.

Patton's still-valid top-secret DOD clearance qualified him to start work as part of the VCF security team. His clearance was provisional—the FBI would have to conduct its own background investigation (as it does for all contract employees) and grant him FBI top-secret clearance. So he was not allowed to see the data the FBI was sending to SAIC, which included information on all of the cases the bureau had digitized to that point, from the 1995 Oklahoma City bombing to 9/11. Instead, he spent a lot of time going through the requirements in his cubicle, segregated from his five colleagues and his boss. He left SAIC in November 2002, after only three months on the job.

Patton regards himself as a straight shooter. "I'm not much of a culture guy," he admits. "I say my piece, and if they don't like it, that's too damn bad."

But he quickly realized that SAIC didn't hire him for his opinions. When he began expressing concerns that security was not a top priority on the project, even in the post-Hanssen era, he was told not to rock the boat.

"My refrain to my boss was, 'Why aren't we more involved? We should be in the thick of things.' But it was more that we weren't really invited and [SAIC teams working on the VCF] aren't actively seeking our involvement," Patton said in an interview in Chicago earlier this year. "So his take on it was basically, once the designers come up with something, we say good, bad, or indifferent, and if it's not too bad, then we let it go."

Patton recounted his experience purely from memory. Unlike Higgins, who meticulously inserted internal FBI e-mails about Trilogy into her scrapbooks alongside photos of her kids visiting her in D.C., Patton said that he discarded the notebook he kept while he was at SAIC. The only existing artifact of his experience is a copy of the 26 October 2002 Internet posting that essentially got him kicked off the VCF project. The posting, archived at http://archives.neohapsis.com/archives/isn/2002-q4/0090.html, expressed specific security-related concerns and depicts SAIC as giving a clueless FBI exactly what it was asking for, no matter how impractical.

Patton's descriptions of the 800-plus pages of requirements show the project careening off the rails right from the beginning. For starters, this bloated document violated the first rule of software planning: keep it simple. According to experts, a requirements document should describe at a high level what functions the program should perform. The developers then decide how those functions should be implemented. Requirements documents tend to consist of direct, general phrases: "The user shall be able to search the database by keyword," for instance.

"In a requirements document, you want to dictate the whats, not the hows," Patton said. "We need an e-mail system that can do x, and there's 12 bullets. Instead, we had things like 'there will be a page with a button that says e-mail on it.' We want our button here on the page or we want it that color. We want a logo on the front page that looks like x. We want certain things on the left-hand side of the page." He shook his head. "They were trying to design the system layout and then the whole application logic before they had actually even figured out what they wanted the system to do."

Recalling the Web pages the agents would bring into the JAD sessions to demonstrate how they wanted the VCF to look, Higgins blamed both SAIC and the agents for creating the overstuffed requirements document. "The customer should be saying, 'This is what we need.' And the contractor should be saying, 'Here's how we're going to deliver it.' And those lines were never clear," Higgins said. "The culture within the FBI was, 'We're going to tell you how to do it.'"

Zalmai Azmi, the FBI's current CIO, has been in that job since December 2003. Originally brought on as a consultant to Mueller that November, Azmi had worked with the director when Mueller was U.S. Attorney in San Francisco and Azmi was CIO of the Executive Office for United States Attorneys. Azmi saw the Virtual Case File through its final death throes. In an hour-long interview in his office at the Hoover Building, Azmi also traced the VCF's demise to flawed requirements and emphasized that his office is taking pains to make sure it doesn't happen again.

Azmi insisted that SAIC should have clarified user needs in the JAD sessions rather than working with requirements that were not "clear, precise, and complete." On the other hand, the FBI's lax project management didn't stop the requirements from snowballing. "There was no discipline to say enough is enough," Azmi said.

The overly specific nature of the requirements focused developers on their tiny piece of the puzzle. They were writing code, Patton said, with no idea of how their piece fit with the others. This presaged the integration problems that would later plague the project.

"The whole working procedure [SAIC project managers] had was very much, 'We'll give you your marching orders and you go,' without too much consideration of how in the world do you glue this sucker back together when all these different divergent pieces come back," Patton said.

Patton also claimed that SAIC was determined to write much of the VCF from scratch. This included an e-mail-like system that at least one team, to his knowledge, was writing, even though the FBI was already using an off-the-shelf software package, Novell's GroupWise, for e-mail. "Every time you write a line of code, you introduce bugs," noted Patton. "And they had a bunch of people slinging code. I'm not saying that the guys were technically incompetent. But bugs happen, and not all programmers are great."

"Every time you write a line of code, you introduce bugs," noted Patton. "And they had a bunch of people slinging code."

After several weeks of asking his boss questions and being repeatedly told that he needed to calm down and be "a team player," Patton posted a message to InfoSec News, an e-mail forum which distributes information security news articles and comments from its subscribers. Without naming the VCF specifically, he mentioned that he was working on Trilogy's case management system and complained that no one was taking security issues seriously. He pointed to some security measures the FBI already had in place that might make the case management system more secure. These included PKI, or public-key infrastructure, a system of digital certificates and independent authorities that verify and

authenticate the validity of each party involved in an Internet transaction. He also mentioned Bedford, Mass.based RSA Security Inc.'s SecurID, which uses a combination of passwords and physical authenticators that function like ATM cards to protect various kinds of electronic transactions.

He asked for help in getting in touch "with some heavy-hitting clued-in people over at the FBI," who would "demand some real accountability from the contractors involved.

"They [the FBI] don't know enough to even comment on a bad idea, let alone tear it apart," he went on. "As a two-bit journeyman I can't seem to get anyone to pay the slightest attention, nor do they apparently (want to) understand just how flawed the whole design is from the get-go."

He ended by asking, "Shouldn't somebody care?"

Somebody did. Sherry Higgins saw the message and promptly reported Patton to the FBI's Security Division. "He had posted information that was not true and was sensitive," she told me in an e-mail. "He was pretty much a disgruntled employee. Instead of bringing his concerns up the ladder, he chose to post them on the Internet. He blasted the team both at SAIC and the FBI."

"Be careful of him," she warned. "In hindsite [sic], I guess it looks like he is saying now, 'I told you so.' However, at the time, he was disruptive instead of constructive."

In response to Higgins's concerns, FBI agents questioned Patton about whether he had disclosed national security information and breached his top-secret DOD clearance.

"There was nothing in there that was sensitive material," Patton maintained. "It was just not flattering of the FBI and the project itself."

After the interview, the FBI decided not to grant Patton top-secret clearance, making it impossible for him to continue working on the VCF. SAIC did invite him to find another position within the company, but it didn't have anything for him in Chicago, to which he was relocating for personal reasons. So at the end of November 2002, Patton left SAIC and the VCF.

That same month the FBI and SAIC agreed to a basic set of requirements, the baseline that SAIC would start from to build the VCF.

In December 2002, Higgins asked lawmakers to invest an additional $137.9 million in Trilogy and the inspector general issued a report on the FBI's management of information technology that included a case study of the program. It found that "the lack of critical IT investment management processes for Trilogy contributed to missed milestones and led to uncertainties about cost, schedule, and technical goals." Apparently unperturbed by the findings, Congress approved another $123.2 million for a project whose total cost had now ballooned to $581 million.

Meanwhile, SAIC programmers were cranking out code. The company had settled on a spiral development methodology, an iterative approach to writing software. Basically, SAIC programmers would write and compile a block of code that performed a particular function, then run it to show Depew's agents what it would do. The agents—some of whom were working at SAIC's data center in Vienna, Va.—gave the programmers feedback, and the programmers tried to incorporate the suggested changes. If there was some dispute as to whether the change could or should be made, the agents sent an official request to the change control board, composed of SAIC engineers and FBI personnel, for review.

It wasn't long before the change requests started rolling in—roughly 400 from December 2002 to December 2003, according to SAIC.

"Once they saw the product of the code we wrote, then they would say, 'Oh, we've got to change this. That isn't what I meant,'" said SAIC's Reynolds. "And that's when we started logging change request after change request after change request." Reynolds added that SAIC's bid on the original contract, and each subsequently revised cost estimate, was based on there being "minimal, minor changes" to the program once a baseline set of requirements had been agreed on. Instead, SAIC engineers were like a construction crew working from a set of constantly changing blueprints.

Some of the changes were cosmetic—move a button from one part of the screen to another, for instance. Others required the programmers to add a new function to a part of the program, such as the graphical user interface, common to all eight development threads.

For example, according to SAIC engineers, after the eight teams had completed about 25 percent of the VCF, the FBI wanted a "page crumb" capability added to all the screens. Also known as "bread crumbs," a name inspired by the Hansel and Gretel fairy tale, this navigation device gives users a list of URLs identifying the path taken through the VCF to arrive at the current screen. This new capability not only added more complexity, the SAIC engineers said, but delayed development because completed threads had to be retrofitted with the new feature. Once SAIC engineers agreed on how the page crumbs would work, one of the development teams created a set of page-crumb-equipped screens for the other seven teams to use as a model. The design model and supporting documentation were updated, the teams made the change—and the schedule slipped

again.

When asked how SAIC programmers reacted to agents' change requests, Depew replied, "Let's just say that we gave them feedback on what they were developing, where it met the requirements and where it didn't. And there was a lot of inconsistency between their development teams."

Higgins was aware that tensions were mounting inside the VCF project over the course of the winter and spring of 2003. Sometimes Depew's team had only two days to review a batch of code. Agents would pull all-nighters to get the evaluation finished, "and in the next iteration their comments wouldn't be taken into account," she said. Sometimes, she acknowledged, these evaluations would include changes to the requirements—functions that the agents had decided that they needed once they saw what they were going to get. Other times the FBI team would find bugs that needed to be fixed.

In March 2003, Computer Sciences Corp., in El Segundo, Calif., which had acquired DynCorp that month, told Higgins that the final deployment of the computers and networks would be delayed until October. In August, October became December. And in October, December became April 2004. The problem wasn't the PCs, which had been trickling in since 2001, but changing the e-mail system from Novell's GroupWise to Microsoft Outlook and, according to the inspector general's 2005 audit, obtaining the components needed to connect the field offices to the wide area network. Higgins added that the delays were compounded by the FBI's own sloppy inventories of existing networks and its underestimation of how taxing the network traffic would be once all 22 000 users came online using their new PCs.

While the FBI and SAIC waited for the networks to go live so they could test the VCF on a real system, changes and fixes continued to strangle the VCF in the crib. Many of the changes had to be to made by all eight of SAIC's development teams. Arnold Punaro, SAIC executive vice president and general manager, admitted in a posting on the company's Web site that in the rush to get the program finished by December, SAIC didn't ensure that all of its programmers were making the changes the same way. That inconsistency occasionally meant that different modules of the VCF handled data in different ways. Consequently, when one module needed to communicate with another, errors sometimes occurred.

"This, however, did not compromise the system," according to Punaro. The real killers, he said, were "significant management turbulence" at the FBI, "the ever-shifting nature of the requirements," and the agents' "trial-and-error, 'We will know it when we see it' approach to development."

Through the summer of 2003, frustration between the agents and the engineers mounted. To quell tensions and discuss design flaws the agents believed were creeping into the VCF, Depew's team asked for a sit-down, what one agent called the "emperor has no clothes" meeting. One Sunday in late September, the agents and the engineers gathered to hash out their differences. Higgins listened in by phone to the first part of the day-long meeting. "There was an awful lot of anger on both sides and a lot of finger-pointing," she recalled. "Nobody's hands were clean." Depew, on the other hand, characterized the meeting as a frank exchange of views. "There was never any animosity shown by my team to the SAIC team," Depew said.

Also in September, the U.S. General Accounting Office (renamed the Government Accountability Office on 7 July 2004) released a report titled "FBI Needs an Enterprise Architecture to Guide Its Modernization Activities." The GAO warned that without a blueprint that provides, in essence, the mother of all requirements documents, the bureau was exposing its modernization efforts, including the VCF, to unnecessary risk.

"I suspect what happened with the VCF is that in the rush to put in place a system, you think you got your requirements nailed, but you really don't," said GAO's Randolph C. Hite, who worked on the report. "It was a classic case of not getting the requirements sufficiently defined in terms of completeness and correctness from the beginning. And so it required a continuous redefinition of requirements that had a cascading effect on what had already been designed and produced."

While stressing that there are no guarantees, Hite believes that "had there been an architecture, the likelihood of these requirements problems would have been vastly diminished."

But the abundantly funded VCF juggernaut was already hurtling toward delivery. SAIC began testing the program in the fall of 2003, and according to Higgins, problems started cropping up, some of which the agents had warned SAIC about over the previous summer. SAIC officials complained to Higgins that Computer Sciences Corp. didn't have its hardware and network in place, so SAIC couldn't adequately test the VCF, crucial for a successful flash cutover. They informed her that they would deliver a version of the VCF to be in technical compliance with the terms of the contract and that the FBI should feel free to make changes to it afterward.

"The feeling was, they knew that they weren't going to make it in December of '03," but they were not forthright about the fact, Higgins said.

On 13 December 2003, SAIC delivered the VCF to the FBI, only to have it declared DOA.

Under Azmi's direction, the FBI rejected SAIC's delivery of the VCF. The bureau found 17 "functional deficiencies" it wanted SAIC to fix before the system was deployed. As an April 2005 report from a U.S. House of Representatives committee pointed out, there were big deficiencies and small ones. One of the big ones was not providing the ability to search for individuals by specialty and job title. Among the small ones was a button on the graphical user interface that was labeled "State" that should have read "State/Province/Territory." SAIC argued that at least some of these deficiencies were changes in requirements. An arbitrator was called in. The arbitrator's findings, released on 12 March 2004, found fault with both SAIC and the FBI. Of the 59 issues and subissues derived from the original 17 deficiencies, the arbitrator found that 19 were requirements changes—the FBI's fault; the other 40 were SAIC's errors.

While SAIC fixed bugs, Azmi, with the help of Depew's team, created investigation scenarios that would take different cases from opening to closing and tested them on the VCF. Those tests revealed an additional 400 deficiencies. "We have requirements that are not in the final product, yet we have capabilities in the final product that we don't have requirements for," Azmi said in an interview.

On 24 March, days after the arbitrator's findings were released, Director Mueller testified to the Senate Committee on Appropriation's Subcommittee on Commerce, Justice, State, and the Judiciary that the VCF would be "on board"—and presumably operational—by the summer of 2004. The director had scant reason to be so optimistic. True, Computer Sciences Corp. was then delivering the final pieces of equipment to the FBI. By April, 22 251 computer workstations, 3408 printers, 1463 scanners, 475 servers, and new local and wide area networks would all be up and running, 22 months later than the accelerated schedule called for. But Azmi and SAIC had yet to agree on the VCF's ultimate fate, much less when it would be deployed. And when SAIC finally offered to take one more year to make all the changes the FBI wanted at the cost of an additional $56 million, Azmi rejected the proposal.

Azmi was promoted from interim to permanent CIO on 6 May 2004. Four days later, the Computer Science and Telecommunications Board of the National Research Council delivered a report on Trilogy that the FBI had commissioned. The "graybeards," as Mueller dubbed them, were led by James C. McGroddy, who had headed IBM Research from 1989 to 1995. The report made two major recommendations. The flash cutover that would start up the VCF and shut down ACS all at once must not happen, as a potential failure would be catastrophic for the bureau. And the FBI should create an enterprise architecture to guide the development of its IT systems. The same committee had made both of these recommendations in September 2002, and according to McGroddy, both suggestions had been ignored until Azmi took charge.

Azmi invited the graybeards to talk with him, Mueller, Higgins, and a few other FBI officials on 20 May 2004. Azmi told the gathering that he had already contracted BearingPoint, where Robert Chiaradio was a managing director and lead advisor on homeland security, to construct the current and future versions of the enterprise architecture by September 2005. And he abandoned the flash cutover idea.

In June, the FBI contracted an independent reviewer, Aerospace Corp., in El Segundo, Calif., to review the December 2003 delivery of the VCF to determine, among other things, whether the system requirements were correct and complete and to recommend what the FBI should do with the VCF. At the same time, Azmi asked SAIC to take the electronic workflow portion of the VCF, code that was in relatively good shape, and turn that into what was eventually called the Initial Operating Capability (IOC), at an additional fixed price to the FBI of $16.4 million. SAIC and the FBI project team had six months to deliver a software package that would be deployed to between 250 and 500 field personnel in the New Orleans field office, the Baton Rouge, La., resident agency, and a drug enforcement unit at the Hoover Building.

The objectives for the new project were clear: test-drive the VCF's electronic workflow; see how people reacted to the graphical user interface; create a way to translate the output from the VCF forms, which was in the eXtensible Markup Language, into the ACS system; check out network performance; and develop a training program. The IOC was the perfect guinea pig for Azmi's rigorous approach to software development and project management, which he called the Life Cycle Management Directive.

The project also needed different managers. On SAIC's side, Rick Reynolds assumed executive oversight on the project from Brice Zimmerman. Reynolds replaced VCF project manager Pat Boyle with Charlie Kanewske. (SAIC declined repeated requests to interview them.) Depew, like other FBI officials, had only good things to say about Kanewske. He had been Kanewske's project manager counterpart for a portion of the Investigative Data Warehouse project, the newest, shiniest tool at the disposal of FBI agents and intelligence analysts. Successfully deployed in January 2004, the warehouse translates and stores data from several FBI databases, including parts of ACS, into a common form and structure for analysis.

But Depew would not be Kanewske's counterpart for the IOC project. He moved back to New Jersey, where he became director of the FBI's New Jersey Regional Computer Forensic Laboratory. When interviewed this past spring, he was overseeing the lab's daily operations and construction of a new wing. He was also anticipating retirement after 31 years of public service and thinking of pursuing job opportunities in the private sector. His final take on the VCF was to the point: "We wanted it really bad, and at the end it was really bad."

As for Sherry Higgins, she went back home to Georgia before the IOC project launched. She now consults and teaches project management courses for the International Institute for Learning Inc., in New York City.

"When it's not fun anymore, Sherry's not a happy girl," Higgins said of her mood just prior to her departure. "The writing was on the wall that IOC was going to be Zal's project. And I just felt like it would be better for me and for Zal for me to leave."

Azmi handpicked his IOC project manager. He chose the bureau's gadget guru (think of "Q" from the James Bond movies)—a man with 20 years of experience delivering surveillance technologies on tight schedules. At a meeting this past May at the Hoover Building, the IOC project manager, whom the bureau made available on condition of anonymity, let me read through an internal FBI report on the IOC and explained the development process in detail. He stressed that the IOC was never meant to be deployed to all 28 000 FBI employees but was intended to test Azmi's methodology. "We followed all of this [process], even in this aggressive timeline, to prove he's got a good framework for managing these projects," he said.

With new management in place, about 120 SAIC engineers began work on the IOC project in June 2004. The FBI and SAIC agreed to keep to a strict development schedule, define acceptance criteria, and institute a series of control gates—milestones SAIC would have to meet before the project could continue.

Azmi, unlike the previous three CIOs, inserted himself into the day-to-day operations of the IOC project. All through the second half of 2004, he met with his project manager every morning at 8:15. Every night before 10 p.m., the project manager would issue a status report indicating what milestones had been hit, identifying risks, and suggesting actions to be taken to avoid mistakes and delays. Azmi's project manager worked closely with Kanewske to adhere to the baseline requirements SAIC and the FBI had agreed on for the IOC in July, thus avoiding a death spiral of change requests. In January, the IOC was rolled out as a pilot right on schedule, and just before the inspector general's stinging critique of the VCF was released.

The report on the VCF from Aerospace Corp., the $2 million study of the December 2003 delivery commissioned by the FBI, began circulating on Capitol Hill at the same time.

[Spectrum's attempt to obtain a copy of the report under the Freedom of Information Act was still being litigated at press time.]

But during a hearing this past 3 February, Senator Judd Gregg (R-N.H.) disclosed that the report said that "the [VCF] architecture was developed without adequate assessment of alternatives and conformance to various architectural standards, and in a way that precluded the incorporation of significant commercial off-the-shelf software." Furthermore, "high-level documents, including the concept of operations, systems architecture, and system requirements were neither complete nor consistent, and did not map to user needs." Finally, "the requirements and design documentation were incomplete, imprecise, requirements and design tracings have gaps, and the software cannot be maintained without difficulty. And it is therefore unfit for use."

The IOC pilot, meanwhile, ended in March. The verdict: "Although the IOC application was an aid to task management, its use did not improve the productivity of most users," according to an internal FBI assessment.

When asked why the IOC did not improve productivity, the FBI project manager emphasized, "The goal was not to achieve improved productivity. What we learned through this is that when they deploy the work flow, there's a need to roll out an electronic records management capability simultaneously."

In other words, FBI employees, particularly agents, found that the IOC actually increased their workload. Why? Agents filled out forms electronically and routed them to superiors for approval, after which the electronic form was uploaded to the ACS, still in use, to be shared with the rest of the FBI. But to comply with the FBI's paper-based records management system, the form had to be printed out, routed, signed, and filed.

So what did the FBI get out of the VCF's last gasp? "We harvested some of the good work from the past," the FBI project manager told me. "We focused that into a pilot. We tested that life-cycle development model of Zal's, and that is a valid, repeatable process. And now we're in a good position to move on."

FBI officials say they are taking what they learned from the VCF and charging ahead with new IT projects on two major fronts. Last September, the White House's Office of Management and Budget tapped the bureau to spearhead the development of a framework for a Federal Investigative Case Management System, an effort involving the National Institutes of Health and the departments of Justice and Homeland Security. The goal here is to provide a guide for any agency in the federal government to use when creating a case-management system.

Then, late last May, Mueller announced Sentinel, a four-phase, four-year project intended to do the VCF's job and provide the bureau with a Web-based case- and records-management system that incorporates commercial off-the-shelf software. Sentinel's estimated cost remains a secret. The bureau expects to award the contract for phase one by the end of this year for delivery by December 2006. SAIC is one of only a handful of

preapproved government contractors eligible to bid on the project.

The FBI's Azmi seems confident that the bureau is ready to handle a project as complex as Sentinel. He said that the FBI has been planning the program for a year, evaluating commercial off-the-shelf software, creating an enterprise architecture, and establishing a number of IT management oversight boards. The bureau has also provided project management training to 80 IT staff members over the last year.

Even so, Ken Orr, an IT systems architect and one of Mueller's graybeards, remains skeptical. He rated Sentinel's chances of success as very low. "The sheer fact that they made that kind of announcement about Sentinel shows that they really haven't learned anything," Orr said, from his office in Topeka, Kan. "To say that you're going to go out and buy something and have it installed within a year, based on their track record," isn't credible.

"They need to sit down and really plan this out, because if they had working software today, they'd have only 25 percent of the problem solved," Orr estimated. The major questions the FBI needs to answer, he contended, include how to bring these new software programs online incrementally and train more than 30 000 people to use them. Then they could focus on converting millions of paper records as well as all of the audio, video, photographic, and physical evidence that has piled up over the years, which will continue to grow at an increasing rate to support the bureau's counterterrorism mission.

"I would guess that it would be closer to 2010 or 2011 before they have the complete system up and running," Orr said. "That's assuming that you have a match between the software and the underlying requirements, which we know are subject to change."

PHOTO: CHAD DOWLING

PHOTO: CLAUDIO VAZQUEZ

PHOTO: DENNIS BRACK, BLOOMBERG, LANDOV

PHOTO: CHAD DOWLING

PHOTO: DAVID STUART

Countdown To Catastrophe

*__September 2000__FBI IT Upgrade Project, later called Trilogy, funded for US $379.8 million.

*__September 2001__Robert S. Mueller III replaces Louis J. Freeh as FBI director a week before the terrorist attacks of 9/11.

*__October 2001__Robert J. Chiaradio advises Mueller on software he dubs the Virtual Case File and brings Larry Depew aboard.

*__January 2002__FBI receives an additional $78 million to accelerate Trilogy.

*__February 2002__Joint Application Development planning sessions begin; Sherry Higgins hired.

*__August 2002__Matthew Patton hired by SAIC as security engineer.

*__November 2002__SAIC and FBI agree on baseline requirements; Patton [above] leaves SAIC.

*__December 2002__FBI receives another $123.2 million to complete Trilogy.

*__September 2003__GAO reports that FBI needs an enterprise architecture.

*__December 2003__Zalmai Azmi becomes acting CIO; SAIC delivers VCF.

*__March 2004__Arbitrator finds that of 59 problems, 19 were FBI changes to requirements and 40 were SAIC errors.

*__June 2004__FBI asks SAIC to develop Initial Operating Capability (IOC) for $16.4 million; FBI contracts Aerospace Corp. to evaluate the VCF.

*__January 2005__Field trials of IOC begin; Aerospace Corp. delivers its report.

*__February 2005__ Final Office of the Inspector General's report on Trilogy comes out; Senate hearing, 3 February.

*__April 2005__ FBI officially kills the Virtual Case File.

*__May 2005__Mueller announces a new software project called Sentinel.

*__December 2005__Contract for phase one of Sentinel to be awarded.