AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–76

FEDERAL BUREAU OF INVESTIGATION'S INFORMATION TECHNOLOGY MODERNIZATION PROGRAM, TRILOGY

HEARING

BEFORE A

SUBCOMMITTEE OF THE

COMMITTEE ON APPROPRIATIONS

UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

SPECIAL HEARING

FEBRUARY 3, 2005—WASHINGTON, DC

Printed for the use of the Committee on Appropriations

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

20–668 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON APPROPRIATIONS

THAD COCHRAN, Mississippi, *Chairman*

TED STEVENS, Alaska
ARLEN SPECTER, Pennsylvania
PETE V. DOMENICI, New Mexico
CHRISTOPHER S. BOND, Missouri
MITCH MCCONNELL, Kentucky
CONRAD BURNS, Montana
RICHARD C. SHELBY, Alabama
JUDD GREGG, New Hampshire
ROBERT F. BENNETT, Utah
LARRY CRAIG, Idaho
KAY BAILEY HUTCHISON, Texas
MIKE DEWINE, Ohio
SAM BROWNBACK, Kansas
WAYNE ALLARD, Colorado

ROBERT C. BYRD, West Virginia
DANIEL K. INOUYE, Hawaii
PATRICK J. LEAHY, Vermont
TOM HARKIN, Iowa
BARBARA A. MIKULSKI, Maryland
HARRY REID, Nevada
HERB KOHL, Wisconsin
PATTY MURRAY, Washington
BYRON L. DORGAN, North Dakota
DIANNE FEINSTEIN, California
RICHARD J. DURBIN, Illinois
TIM JOHNSON, South Dakota
MARY L. LANDRIEU, Louisiana

J. KEITH KENNEDY, *Staff Director*
TERRENCE E. SAUVAIN, *Minority Staff Director*

SUBCOMMITTEE ON COMMERCE, JUSTICE, AND STATE, THE JUDICIARY, AND RELATED AGENCIES

JUDD GREGG, New Hampshire, *Chairman*

TED STEVENS, Alaska
PETE V. DOMENICI, New Mexico
MITCH MCCONNELL, Kentucky
KAY BAILEY HUTCHISON, Texas
SAM BROWNBACK, Kansas
THAD COCHRAN, Mississippi
(ex officio)

DANIEL K. INOUYE, Hawaii
BARBARA A. MIKULSKI, Maryland
PATRICK J. LEAHY, Vermont
HERB KOHL, Wisconsin
PATTY MURRAY, Washington
ROBERT C. BYRD, West Virginia
(ex officio)

Professional Staff
KATHERINE HENNESSEY
DENNIS BALKHAM
JILL SHAPIRO LONG
JESSICA ROBERTS
NANCY PERKINS
CHAD SCHULKEN *(Minority)*
KATE ELTRICH *(Minority)*

CONTENTS

FEDERAL BUREAU OF INVESTIGATION'S INFORMATION TECHNOLOGY MODERNIZATION PROGRAM, TRILOGY

THURSDAY, FEBRUARY 3, 2005

U.S. SENATE,
SUBCOMMITTEE ON COMMERCE, JUSTICE, AND STATE,
THE JUDICIARY, AND RELATED AGENCIES,
COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 2:01 p.m., in room SD–192, Dirksen Senate Office Building, Hon. Judd Gregg (chairman) presiding.

Present: Senators Gregg, Stevens, Mikulski, and Leahy.

OPENING REMARKS OF SENATOR JUDD GREGG

Senator GREGG. The subcommittee will come to order. I appreciate Senator Leahy being here. We haven't really organized as an Appropriations Committee yet, so we do not know who is chairman of what and who is ranking where, but for the moment, Senator Leahy is serving as the acting ranking member for this subcommittee. It is nice to have my neighbor and friend from across the river, as we refer to it, sitting here as the Democratic leader on this committee.

This hearing is called, regrettably. I wish it wasn't being held. I know the Director wishes it wasn't being held and the Bureau does, also, I am sure.

For a long time, this committee has committed a large number of resources, a tremendous amount of effort, on working with the Federal Bureau of Investigation (FBI) to try to upgrade the technology capability of the agents on the street and the FBI generally, not only within the Bureau but as it integrates with the rest of the Government, especially on this core issue of how we fight terrorism. Part of this initiative, of course, has been the famous Trilogy program, which has had fits and starts, which has involved a large number of dollars and in which we have made a serious effort.

The FBI, to begin with, needs to be congratulated. We are 3½ years out from 9/11 and we haven't been attacked, and that is in large part because of the excellent work of the FBI and the men and women of that agency who commit their lives to making sure that we are secure. I congratulate the Bureau for that and the American people thank you for it.

TRILOGY PROGRAM SOFTWARE

In addition, there have been some successes with the Trilogy program that deserve praise. The bringing online of the hardware was done on time and it appears to be well done.

But the big issue is the software which runs the hardware. Here, we have a huge problem. It has been reported that we now have independent evaluations and it appears that the Virtual Case File (VCF) element, which is essentially the software which would give the agents and the FBI the capacity to adequately consolidate and track cases from agent to agent, from field office to field office, from central command back to field offices, has failed catastrophically.

And so we have got to address why it failed, first. Second, we have to ask the question of who is responsible. I think that is only reasonable because there is a large amount of taxpayers' dollars that have produced very little for the taxpayers, over $100 million minimum. And then, third, where do we go from here, because this is a critical element of having an efficient and effective FBI and especially an efficient and effective deterrent to terrorism. So now that we have had this very significant failure, how do we get back on track and what is the timeframe, what is the cost, and most importantly, can it be done?

The Director has kindly agreed to come and testify today. I appreciate his courtesy in giving us time today on this issue. We are going to proceed with trying to find out what is going on and how we can fix the problem. We are not too interested in spending a lot of time on the history of the blame. We are more interested in figuring out how we fix the problem.

Senator Leahy.

OPENING REMARKS OF SENATOR PATRICK J. LEAHY

Senator LEAHY. Thank you, Mr. Chairman. I agree very much with what you had to say. Mr. Chairman, perhaps it is our New England upbringing that we get somewhat worried about the amount of money that has been put in here and will never be recovered.

We have an important issue for the FBI in this. I am glad that Director Mueller and Inspector General Fine have returned to testify. I appreciate the time Director Mueller spent with me yesterday, he and Mr. Azmi and others. I made very clear to him my concern at that time on this and some other subjects.

POSSIBILITY OF SCRAPING KEY TRILOGY COMPONENTS

I know Groundhog Day was yesterday, but I think of that movie, "Groundhog Day," and the sense of dèjá vu the movie had. It is unbelievable, given the years that have gone by, the advances in technology that have marched on in the meantime, that we are here today to discuss whether or not to completely scrap a key component of the Trilogy project, the long-anticipated Virtual Case File. It has been kind of a train wreck in slow motion, unfortunately, at a cost of $170 million to the taxpayers, or a very large part of that. We don't know how much of a cost to the public.

I don't want New England reserve to fool anybody to think that my reaction getting the initial reports of this was much short of ap-

oplectic, this unraveling of the Trilogy project, or as some FBI agents have told me privately, the tragedy project. It would bring the FBI's information technology into the 21st century. That shouldn't be rocket science. Most companies have to do that. It should be doable.

This has been a long and tortured effort. Back in 2000, when we began discussions about Trilogy as a way to bring the FBI's antiquated system into the 21st century, we were warned of dire consequences to our security and our safety if the improvements weren't imminent, if we didn't give them the money so that it could be done right away. Well, we responded. We devoted $581 million to the project.

ASSESSMENTS OF VISUAL CASE FILES

But time and again, it has fallen victim to escalating costs and implementation concerns, mismanagement, and so on. The estimated December 2003 deadline for completion of it passed unmet. The program was then dubbed unusable. We now know that it is being tested as the so-called "Virtual Case File (VCF/Light)."

The $170 million seems to have evaporated. Maybe some of this, we can get back from those supplying software and hardware. But what bothers me is that a lot of the delays in communications, even though we asked in different committees—and I am on the authorizing committee as well as the appropriating committee—we never seemed—they weren't communicated to Congress, and it wasn't because Republicans and Democrats alike weren't asking. We were.

The FBI has repeatedly pressed for realistic assessments of VCF, but getting straight answers from the Department of Justice and the FBI have proved so difficult that we finally turned to the Government Accountability Office (GAO) for an independent assessment. It is only in the shadow of that impending Office of Inspector General (OIG) report that suddenly this comes to light. We have a classic example of too many cooks with the unpredictable results.

The initial contract for VCF was modified 36 times. During this period, the FBI had five different chief information officers, I am told 10 different project managers. Beyond that shuffling, several teams were brought into the process at various times to help set requirements, assess deliverables, and manage costs. Even the efforts of the GAO have been thwarted by changes in personnel and trying to get answers.

Technology changes rapidly, I appreciate that. But the private sector has to make these decisions under similar pressures and it is not too much to demand the same from the FBI.

The September 11 attacks did change the FBI's assessment on what is needed. I appreciate that. But 3 years have passed for the FBI to regroup. The Congress has responded with the necessary financial resources.

LESSONS LEARNED

Now, this has been a very, very expensive lesson learned program. Congress paid for something to be built, not for learning what has to be built through trial and error. We have to protect the American people. To do this effectively, the FBI has to have state-of-the-art technology that works. It is a vital task. Now we

are going to have to spend more money to buy what we thought we bought.

But I think that just simply spending money is not going to be enough. We can't just keep throwing money at the problem. I think that the FBI has got to stop hiding its problems. The Department of Justice has to stop hiding its problems. You know, you have a lot of us up here who have been very, very supportive of law enforcement, very supportive of the FBI. I have done this for 30 years in both appropriations and authorizations. But, you know, the camel's back is broken, and if you think that some of us who have been supportive in the past are going to keep on spending money and we are not getting answers, or are told all is well when it is not, it is just not going to work.

Mr. Chairman, I agree with you. It is unfortunate we have to be having this hearing, but thank goodness we are.

Senator GREGG. Thank you.

[The statement follows:]

PREPARED STATEMENT OF SENATOR PATRICK J. LEAHY

I commend Chairman Gregg for convening this hearing today. This is an important issue for the FBI and its missions in protecting the country, and I appreciate the opportunity to serve as ranking member on this hearing. I am pleased that both Director Mueller and Inspector General Fine have returned to testify, I welcome them and the other witnesses, and I look forward to their testimony.

I know that Groundhog Day was actually yesterday, but the subject of today's hearing—problems the FBI is having with its computers—calls to mind the sense of déjà vu that the film of the same name captured so well. It is unbelievable given the years that have gone by and the advances in technology that have marched on in the meantime that we are here today to discuss whether or not to completely scrap a key component of the FBI's Trilogy project—the long-anticipated Virtual Case File. This program has been a train wreck in slow motion, at a cost of $170 million to American taxpayers and an unknown cost to public safety. And sadly, VCF is but one of many Trilogy problems at the FBI.

Apoplectic would be too mild a description of my reaction to the unraveling of the Trilogy project—or the Tragedy project, as some FBI agents have taken to calling it. Bringing the FBI's information technology into the 21st Century should not be rocket science; it is a complicated process, but it is certainly doable.

The history of the FBI's efforts to upgrade its information technology has been long and tortured. Back in 2000, when we began discussions about Trilogy as a way to bring the FBI's antiquated systems into the 21st Century, we were warned of dire consequences to our security and our safety if the improvements were not imminent. The picture was bleak. The Bureau had no functional e-mail system at the time, and over 13,000 desktop computers that were years old could not run basic software packages. Congress responded by devoting $581 million to the effort.

These deficiencies had real-world consequences, hampering the FBI's ability to share important and time-sensitive information internally and externally with other intelligence and law enforcement agencies. In testimony before the Senate Judiciary Committee, 9/11 Commissioner Slade Gorton noted: "[I]nformation technology problems . . . have hampered the FBI's ability to know what it knows for years" and led to the now infamous incident of the Phoenix memo on terrorists and flight schools that never made it to the attention of top officials who should have seen it.

Time and again, the project has fallen victim to escalating costs, imprecise planning, mismanagement, implementation concerns, and delays. The necessary network, hardware and software upgrades were not delivered in a timely manner. Consequently, the estimated December 2003 deadline for completion of VCF passed unmet. The program was then dubbed "unusable," and we now know that what is being tested is a significantly scaled-down version, a so-called "VCF-lite." And in keeping with the past disappointments and delays, we have recently learned that the future of this "lite" version remains in question.

Congress was led to believe that VCF was progressing on track despite some delays and cost overruns on the project. Yet now we hear that VCF may never be completed at all. In effect, that means for Congress, for the FBI and, most impor-

tantly, for the American taxpayer, this has been $170 million in "vaporware"—widely advertised, but never actually available for use.

There has been no shortage of opportunities for straightforward reporting to the oversight committees of Congress as things began to come off the tracks, including numerous hearings, punctuated by several damaging reports from OIG, the Government Accountability Office, and the National Research Council. These delays and disappointments were never communicated to Congress, and it is not because Congress failed to ask. The FBI was repeatedly pressed for realistic assessments of VCF. But getting straight answers from the Justice Department and the FBI proved so difficult that Congress finally turned to the Government Accountability Office for an independent assessment. It was only in the shadow of an impending OIG report that the reality of the situation has come to light.

Director Mueller testified before the Judiciary Committee last May and was specifically asked about the status of VCF. He testified then that "we are on track to deliver elements of virtual case file capabilities by the end of this year. We are in negotiations with our contractor on finishing out that last part of the Trilogy project . . . But I do believe that when we are concluded this year, we will have the foundation for cutting-edge technology for an organization our size."

What was not presented in this hearing was any acknowledgement or even any hint that progress had halted and the project was, in fact, falling apart. This was an opportunity for Director Mueller to show some accountability and be upfront with Congress about the problems with the project. The FBI missed another opportunity to come clean three months later when the Committee convened a hearing on the 9/11 Commission's recommendations.

It appears the FBI bears the brunt of the responsibility for this derailment; a classic example of too many cooks, with the predictable results. The initial contract for VCF was modified 36 times. During this period, the FBI had five different Chief Information Officers and, reportedly, 10 different project managers. Beyond all that shuffling at the top, several teams were brought into the process at various times to help set requirements, assess deliverables and manage costs. Even the recent efforts of the GAO to audit the project have been thwarted by repeated changes in the personnel responding to auditors' inquiries.

It is not clear to me even yet what the FBI truly knew and whether the Bureau articulated what it needed, though initial reports suggest the FBI made an art form of redefining and changing its requirements. The project's contractor, Science Applications International Corporation, has said it received changes on almost a daily basis—some small, but many, significant. Unbelievably, the OIG reports that the process for defining the requirements and baselines for the VCF continues to this day. I look forward to hearing from Inspector General Fine on this matter. The Trilogy project is reminiscent of other FBI technology failures where the Bureau has ambitiously tried to build the latest and greatest without properly assessing its needs. The FBI custom-built the Carnivore system on the basis that it was "far better" than any commercial product, but after very little use, recently scrapped it for an undisclosed commercial product.

Technology changes rapidly, and I appreciate the FBI's efforts to keep pace. But the private sector has had to make these hard decisions with similar pressures, and it is not unreasonable to demand as much from the FBI. The September 11th attacks did change the FBI's assessment of what it needed. But three years have passed for the Bureau to regroup, and in that time Congress has responded with the necessary financial resources to assist the Bureau in adapting in these tasks. This has been an outrageously expensive lessons-learned training program. Congress paid for something to be built, not for learning about what to build through trial and error.

I am aware of the concerns that have also been raised about the performance of SAIC, the project's contractor, and I do expect SAIC to account for any failures in its work product.

Our highest priority must be to protect the American people. To do its job effectively, the FBI must have state-of-the-art technology that works. This is a vital task, and now Congress will have to provide still more funding to get the job done. But throwing money at this chronic problem alone will not fix it. The FBI must stop hiding its problems and begin confronting them. The FBI needs to engage in a full working partnership with the authorizing and appropriations committees to which the Bureau is accountable to for programs like this. Doing that will better protect the public, conserve tax dollars, and save everyone's time.

The camel's back is broken. For a course correction to succeed, there must be a true accounting, and it is going to start today. We want to hear what went wrong, who was responsible, and how we are going to move forward.

Senator GREGG. Traditionally, we haven't had opening statements beyond the chairman and the ranking member, but obviously, participation today is by folks who are really interested in this and I didn't know whether you wanted to make a statement.

STATEMENT OF SENATOR BARBARA A. MIKULSKI

Senator MIKULSKI. Just very briefly, Mr. Chairman. First of all, I want to thank you for holding this hearing. You have always stood sentry over getting taxpayers' value for taxpayers' dollar, and you were the first to hold public hearings on the issue of terrorism, so we thank you for your leadership.

Also to Senator Leahy, in the absence of a permanent Chair of CJS, we thank you for filling in. It is also very possible that if the draconian restructuring program of the House would ever go through, I might Chair this subcommittee, which——

Senator GREGG. Or be ranking.

Senator MIKULSKI. Or just be ranking.

Oh, no, that is another restructuring.

Senator LEAHY. I wasn't going to say a word.

Senator MIKULSKI. I am sorry.

Senator LEAHY. I am just staying out of this one.

Senator MIKULSKI. I am sorry. I was so excited. That was regime change, not restructuring.

But I also wanted to be here as a member of the committee. I am a member of the Intelligence Committee. We went through the 9/11 inquiry and we were absolutely very clear that our FBI needed to modernize itself. We are proud of the FBI and we are proud of the fact that we have asked them to retool their mission, retool their people, and retool their technology. And now, as we have moved forward to the reform necessary for both intelligence and FBI, I think the Director is working very hard on this retooling of the mission. The people that he has hired have helped him do this. Now we have to make sure that we have the right technology to do this.

TECHNOLOGY PROGRAMS GOING BUST

Right after 9/11, we found out that the FBI had 13,000 desktop computers that were outdated and dysfunctional. We also saw that that whole idea of watch lists talking to each other, offices talking to each other, and so on was outdated. We have got to get this back on track.

As someone who has looked at these big technology programs, whether it was in transportation, whether it was out of the VA/HUD Subcommittee, they have always been a bust. I think maybe we have to reexamine that rather than inventing things, that we need to look at how to buy things off the shelf, how we can move quicker, faster, cheaper, and save a lot of heartache, a lot of heartburn, and a lot of taxpayers' dollars.

But I know today is the day for getting the FBI and its financial and computer programs back on track and I look forward to working with you in any capacity in which I might find myself.

Senator GREGG. I look forward to that, also.

Senator MIKULSKI. I am ready to retool if I have to.

Senator GREGG. Mr. Director, we are ready to hear your thoughts and explanations.

STATEMENT OF HON. ROBERT S. MUELLER, III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE

ACCOMPANIED BY ZALMAI AZMI, CHIEF INFORMATION OFFICER, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE

OPENING STATEMENT OF DIRECTOR MUELLER

Mr. MUELLER. Thank you, Mr. Chairman, Senator Mikulski, Senator Stevens. I do want to thank you, believe it or not, for the opportunity to be here today to discuss this issue because it is important. It is important to the Federal Bureau of Investigation (FBI), it is important to the country, and I know it is important to the Congress.

I do want to spend some time discussing the questions that you, Mr. Chairman, have raised. As all of us know, the Virtual Case File is a case management system constituting the third prong of the FBI's mission technology program and is known as Trilogy. It was first developed in 2001.

COMPLETED PHASES OF TRILOGY

I want to point out at the outset that the first two phases of Trilogy have been successfully completed and, as the chairman pointed out, have been deployed and have greatly enhanced our information technology capabilities. We now have deployed a high-speed network enabling our FBI offices around the country and around the world to share data, including audio, video, and image files. Our new IT infrastructure also provides for secure communications with our intelligence community partners.

We have replaced those outdated computers with more than 30,000 new desktop computers with modern software applications, and we have replaced nearly 4,000 printers. We have 1,600 scanners, 465 servers, and as important, 1,400 routers that have been installed.

As a result of the implementation of the first two prongs of Trilogy, FBI personnel can now utilize a uniform suite of software that enables our agents and our support to share information quickly, reliably, and securely.

These efforts have also provided a foundation for a number of new capabilities to support the FBI's counterterrorism mission. I will point out at the outset that after September 11, while Trilogy and bringing Trilogy home was tremendously important, it also at that time was critically important to us to take our counterterrorism information throughout the Bureau, information from elsewhere on counterterrorism, and place that information in an updated investigative data warehouse. We now have that information, that investigative data warehouse, that has that information and provides to special agents, intelligence analysts, and members of joint terrorism task forces a single access point to more than 47 sources of counterterrorism data that was only in the past available through separate stovepiped systems.

We have new analytical tools used across multiple data sources, providing a more complete view of the information possessed by the

Bureau. Users can now search up to 100 million pages of international terrorism-related documents and other structured records, such as addresses and phone numbers, in seconds. They can also search rapidly for pictures of known terrorists and match or compare the pictures with other individuals in minutes rather than days.

CRITICAL IT IMPROVEMENTS

Other critical IT improvements have enabled the FBI to proceed with unprecedented connectivity with our partners in the intelligence and law enforcement communities. The SCION network gives FBI personnel the ability to electronically receive, disseminate, and share compartmented sources of intelligence information amongst our various operating divisions and with the intelligence community.

But despite these significant improvements, the Virtual Case File, which is a case management application for improving efficiency and records management, is not yet available to our personnel. I can tell you, Mr. Chairman, as I have expressed in private to yourself and Senator Leahy, there is no one who is more frustrated, no one who is more disappointed than I at the delays we have encountered in deploying VCF. I do believe, however, it is important to the American people to understand what the failure to deliver VCF means, and what it does not mean, to the FBI agent on the street.

TECHNOLOGY FOR STREET AGENTS

I want to point out that the FBI agent on the street has the state-of-the-art technology when it comes to surveillance. Without getting into sensitive and classified information, I can assure you that our ability to intercept and decipher communications and to otherwise monitor criminal activity and gather intelligence is among the best in the world. The FBI agent on the street is able to communicate and share data securely, whether by telephone, computer, or teleconference with our partners, not only in the FBI but also in the law enforcement and intelligence communities in the United States and around the world.

What the agent on the street does not have is a user-friendly format for inputting investigative and intelligence information into his or her computer. Instead, the agent faces a cumbersome, time-consuming process of preparing a paper record of that information, seeking the necessary approvals, and then uploading that document into an existing database. If the agents had the Virtual Case File capabilities we had envisioned, they could directly input information into their computers, receive electronic approvals, and with the push of a button upload information into the database where it would be immediately available to others who need to access it, whether it be an agent, an analyst, or other Federal employees and State and local officials.

And by saying this, Mr. Chairman, I do not mean to say that this does not affect our capacity to protect the United States. To the extent that we are delayed, to the extent that we do not have this Virtual Case File, we are not as effective or efficient as we should

be in protecting the people of the United States, whether it be from terrorism or criminals within the country.

VIRTUAL CASE FILE ANSWERS

Mr. Chairman, this afternoon, I would like to take this opportunity to answer the three basic questions about Virtual Case File which you elucidated in your opening statement. First of all, what went wrong? Second, who is responsible for what went wrong? And third, where do we go from here?

What went wrong? The development of the VCF application started with a relatively simple concept that the FBI needed a modern case management system. As the FBI's mission evolved, particularly over the past 3 years, so did our technological needs. And as a result of these changes and other issues, the FBI faced obstacles in a number of key areas relating to the VCF program.

We did not have a complete set of defined VCF requirements when the original contract was signed in June 2001, and we did not have a finalized set until the summer of 2002.

The contract which we entered into was based on hours worked, a cost plus award fee, and we now know that these types of contracts are difficult to manage.

But from our perspective, we also lacked skill sets in our personnel, such as qualified software engineering, program management, and contract management.

We underestimated the complexity of interfacing with our legacy systems, of addressing our security needs, and of establishing an enterprise architecture.

Recognizing many of those internal limitations originally, we did decide to outsource the development of VCF, including contract management and technology development. The contractor responsible for delivering the user applications component, including VCF, was Science Applications International Corporation (SAIC). I know you are to hear from them today, as well.

Following the establishment of the solid requirements in November 2002, the original target date for completing VCF was December 2003. I personally received a demonstration of the VCF software in November 2003, and was impressed by what I saw at that time. I anticipated that we would be moving forward expeditiously to the installing of that VCF on our agents' support computers in the relatively near future once we had upgraded all of our computers from a Windows 98 operating system to a Windows 2000 operating system. I, at that time, believed that we were on the right track to deliver that which our employees were seeking.

When SAIC delivered the first product in December 2003, we immediately identified a number of deficiencies, 17 at the outset. That soon cascaded to 59 and ultimately to 400 problems with that software. In April 2004, we provided SAIC with a document outlining the corrections we felt were needed and SAIC ultimately agreed to remedy the deficiencies and deliver full functionality, but only at a cost, an additional $56 million, and a timetable, an additional year, which at that time we had problems with.

TWO-TRACK VISUAL CASE FILE PLAN ADOPTION

So in June 2004, I decided to adopt a new two-track plan for VCF, an initial operating capability, or IOC, and a full operating capability, which is denominated as FOC. My goal with the IOC was to identify and utilize some portion of the product developed by SAIC since the fully functional case management system as we had anticipated had not been delivered. The portion of Virtual Case File currently being piloted is the automated workflow process. Last month, several hundred employees in the New Orleans field office began using the system as their document routing system and will continue to do so through the end of March.

The purpose of this pilot is to test drive the workflow concept, validate the human-computer interface, create an electronic interface to our legacy systems, access the network performance, and develop and deliver an enterprise-level training curriculum. The IOC, the initial operating capability, is on track to accomplish these objectives.

As part of two-track plans, the FBI contracted with multiple independent vendors to perform the following tasks: Examine the Virtual Case File application delivered by SAIC in December 2003, to determine if this software, as designed, would meet the FBI's operational, security, and performance requirements. Aerospace Corporation was tasked to determine if the Virtual Case File application is scalable and can be maintained and enhanced easily.

They were also asked to examine the current technologies and vendors as well as available commercial off-the-shelf or COTS, products. They were also tasked to look at those products designed for other agencies to determine the best combination to meet the FBI's needs. This effort was conducted jointly, not only with ourselves and the Department of Justice, but also with the Department of Homeland Security, to ensure our case management efforts would be interoperable. In many ways, as several of you have pointed out, the pace of technological innovation and the need for information sharing has overtaken our original vision for Virtual Case File and there are now products to suit our purposes that did not exist when Trilogy was first envisioned.

We have also asked a different contractor to review and revalidate our users' requirements because the mission of the FBI has evolved and there are new requirements for information and intelligence sharing among different entities.

Last week, we received the final version of the Aerospace report and provided copies to this subcommittee and to the Office of Inspector General at the Department of Justice.

RESPONSIBILITY FOR WHAT WENT WRONG

Question number two, who is responsible for what went wrong? Mr. Chairman, I am responsible, at least in part, for some of the setbacks experienced with Trilogy and Virtual Case File. I agree with the OIG's findings that FBI management did not exercise adequate control over the Trilogy project and its evolution in the early years of the project.

Let me also add that I agree with the OIG's finding that with the new organizational structure and authority given to the Chief

Information Officer (CIO), Zal Azmi, in July 2004, project management has now been given the attention that was needed throughout the Trilogy project. Zal Azmi is here with me today. He started with me as a special advisor on technology issues when I first saw problems in the fall of 2003. He became the Chief Information Officer in spring of last year, and through his leadership, the FBI has implemented a coordinated strategic approach to information technology. My prepared statement outlines a number of the steps that Mr. Azmi has taken as CIO and some of the accomplishments of him and the people with whom he works.

I also will say, and I think it is shared in the testimony from SAIC, that in addition to our shortcomings in overseeing the Trilogy project, the contractor also bears some responsibility. As discussed above, we retained a not-for-profit federally funded contractor, Aerospace Corporation, to conduct an independent verification and validation review of the Virtual Case File, the VCF software as delivered by SAIC in December 2003.

Aerospace in its report concluded that, and I quote, "lack of effective engineering discipline has led to inadequate specification, design, and development of VCF." In the course of their review, Aerospace could find no assurance that the requirements were satisfied nor that the architecture concept of operations and requirements were correct and complete. When we received this report recently, we were indeed disappointed.

VIRTUAL CASE FILE FUNDING

With regard to the funding of Virtual Case File, this committee has been supportive of our efforts and has generously provided the funding we have needed to overcome obstacles and attempt to move forward. Mr. Chairman, you and other members are undoubtedly concerned, as am I, about losses we have incurred as well as future investments we will need to make in Virtual Case File.

We have invested approximately $170 million in VCF to date. It is my understanding that our vendors have delivered services and reusable equipment worth $53.3 million and that we have $12.2 million in unspent obligations on our VCF contracts. This results in a loss of approximately $104.5 million. I do not take that lightly. It is $104.5 million that we will not have to spend on other things. It is $104.5 million of the taxpayers' dollars and I am tremendously troubled by that and that is an understatement. I am disheartened by this result, but remain confident in our ability now to deliver a case management system to our employees' desktops in the future.

WHERE DO WE GO FROM HERE

Last question, where do we go from here? The development and deployment of an investigative case management system remains the top priority of the Office of the Chief Information Officer. Some components of VCF that have been developed will be incorporated into the long-term solution. We will leverage the permanent interface that has been established with our legacy data systems. We will assess the impact of an automated workflow system on a field office and headquarters structure as well as the performance of a case management system on the new Trilogy network, during, and

at the end, of the pilot testing period. We will take with us a number of valuable lessons learned in contract management, project management, policies and procedures, modular development and deployment, data security, and records management.

Not surprisingly, the pace of technology has overtaken the development of unique software applications for the Bureau and we may turn to commercial off-the-shelf, or COTS-based products, to give us that which we had envisioned in Virtual Case File. We are currently reviewing the Aerospace reports which recommend that we discard VCF and start over with a COTS-based product and which provide their evaluation of COTS products as well as products in use by other Government agencies. As we review these reports, we will continue to consult with industry leaders to ensure that we develop a sound long-term plan for our IT needs.

We will move forward with a phased, and I emphasize a phased, development and deployment plan as recommended by the National Academy of Sciences. Every phase will provide a set of services that the FBI workforce needs and which was part of the original VCF plan.

I cannot at this time estimate when this will occur, nor can I determine right now what we will need in terms of additional funding. I will tell you that we will work closely with this committee and other committees of Congress to develop the future for a Virtual Case File, and with the work of Mr. Azmi and the people he has brought in, with input from persons outside the Bureau, I am confident that we, in a phased way, can replicate that which we had envisioned in 2000 and 2001 as being a part of Virtual Case File.

AEROSPACE CORPORATION SELECTION

Mr. Chairman, before I conclude, let me say that I have reviewed the testimony of other witnesses and there are two questions that I would anticipate and would like to answer at the outset.

The first question is, how did we select Aerospace Corporation to conduct the independent verification and validation review, and I am going to pass that over to Mr. Azmi.

I am going to start on the second question, and that is why did we limit Aerospace's review to the December 2003 delivery of Virtual Case File and not include that which was produced in December 2004 and that which we are testing now.

I will tell you, last spring, in 2004, after we saw the problems we had in the version that was provided in December 2003, we entered into negotiations with SAIC, and at the end of those negotiations it was clear from their leaders that we would have to invest another $56 million and an additional year of time to complete the project as we had anticipated with SAIC. At that time, in consultation with Mr. Azmi, I felt we needed an independent review of the work that had been produced by SAIC and that is the version that we had to review at that time. I am comfortable in having Aerospace or anyone else review the initial operating capacity that is currently being tested in New Orleans and here at the FBI headquarters.

Mr. Azmi may want to provide more input into why we asked Aerospace to review the December 2003 delivery, and I would also

ask him to answer the question as to why we selected Aerospace, because I believe that is when it would be forthcoming, and then I will close.

Mr. AZMI. Mr. Chairman and members of the committee, thank you for the opportunity to appear here today and respond to your questions.

On the question, why we selected Aerospace to conduct an evaluation of the VCF delivery of 2003, it was mainly a recommendation made by the Director of the Science Board. When I arrived in November 2003, I realized that the Director already had a number of boards and advisors that were actually providing input to the future of the information technology within the Bureau. I met with the Science Board—the members are former CIOs, technologists from both the Government and private sector—and I presented the dilemma that we were facing with VCF.

The software was delivered with 17 deficiencies. We decomposed those 17 deficiencies to 59. Later on, we found 400 problems with the software, and that was the recommendation of the Board, that we conduct an independent evaluation.

We had selected three sources of evaluators. Aerospace was selected because it was a federally funded organization, a nonprofit organization. It had worked with the Department of Defense (DOD) and the intelligence community for more than four decades. They were also capable of providing in-depth software engineering review that we needed. For those reasons, we selected Aerospace to conduct an independent evaluation of the VCF software. Thank you, sir.

Mr. MUELLER. Anything to add on why we selected the December 2003 version to be evaluated?

Mr. AZMI. I can add only one point. When I arrived, I looked at the contract and the contract stated specifically that SAIC will deploy a working version of VCF by December 17, 2003. When I looked at all of the capabilities of VCF, what should have been delivered and what was delivered, we decided if we are going to invest in the software for the future of the FBI, if we will have to stay with this software, we need to understand what the software will provide to us, and that is one of the reasons why we selected to evaluate that software that was promised to the Bureau from the outset of support of this contract.

PREPARED STATEMENT

Mr. MUELLER. So in closing, those hopefully answer the questions that would have been asked. I want to thank the subcommittee, you in particular, Mr. Chairman, for your support throughout this endeavor, your patience, understanding your frustration. Mr. Azmi and I are happy to respond to any questions that the subcommittee may have.

Senator GREGG. Thank you, Mr. Director, and thank you for your forthrightness.

[The statement follows:]

PREPARED STATEMENT OF ROBERT S. MUELLER, III

Good afternoon, Mr. Chairman, Senator Leahy, and Members of the Committee. Thank you for the opportunity to appear this afternoon and address concerns relat-

ing to the FBI's Virtual Case File system, or VCF. As you know, VCF is a case management system constituting the third prong of the FBI's information technology program known as Trilogy. The first two phases of Trilogy have been successfully completed and deployed, and have greatly enhanced our Information Technology (IT) capabilities.

—We have deployed a high-speed, secure network, enabling personnel in FBI offices around the country and around the world to share data, including audio, video and image files. Our new IT infrastructure also provides for secure communications with our Intelligence Community partners.

—We have also replaced outdated hardware with more than 30,000 new desktop computers with modern software applications, nearly 4,000 new printers, 1,600 scanners, 465 servers, and 1,400 routers.

As a result of the implementation of two major prongs of the Trilogy initiative, FBI personnel can now utilize a uniform suite of software that enables them to share information quickly, reliably, and securely. These efforts have also provided a foundation for a number of new capabilities to support the FBI's counterterrorism mission. The new capabilities include:

—The FBI's Investigative Data Warehouse (IDW) now provides Special Agents, Intelligence Analysts, and members of Joint Terrorism Task Forces (JTTFs) with a single access point to more than 47 sources of counterterrorism data, including information from FBI files, other government agency data, and open source news feeds, that were previously available only through separate, stovepiped systems.

—New analytical tools are used across multiple data sources providing a more complete view of the information possessed by the Bureau. Users can search up to 100 million pages of international terrorism-related documents and other structured records such as addresses and phone numbers in seconds. They can also search rapidly for pictures of known terrorists and match or compare the pictures with other individuals in minutes rather than days. Coupled with sophisticated state-of-the-art search tools, the IDW enhances the FBI's ability to identify relationships across cases quickly and easily.

—Other critical IT improvements have enabled the FBI to proceed with unprecedented connectivity with our partners in the Intelligence and Law Enforcement Communities. The Top Secret/Sensitive Compartmented Information Operational Network (SCION) gives FBI personnel the ability to electronically receive, disseminate, and share compartmented sources of intelligence information among the FBI's counterterrorism and counterintelligence operations and with the Intelligence Community. SCION also provides for video teleconferencing at the TOP SECRET level.

Despite these significant improvements, the Virtual Case File—a case management application for improving efficiency and records management—is not yet available to our personnel. Mr. Chairman, no one is more frustrated and disappointed than I at the delays we have encountered in deploying VCF. But I believe it is important for the American people to understand what the failure to deliver VCF means—and what it doesn't mean—to the FBI Agent on the street.

The FBI Agent on the street has state-of-the-art technology when it comes to surveillance. Without getting into sensitive and classified information, I can assure you that our ability to intercept and decipher communications and to otherwise monitor criminal activity and gather intelligence is among the best in the world. The FBI Agent on the street is able to communicate and share data securely, whether by telephone, computer, or teleconference with our partners, not only in the FBI, but also in the law enforcement and intelligence communities, in the United States and around the world. The Agent on the street is able to access FBI documents electronically on our existing computer systems and to search those documents using multiple search technologies.

What the Agent on the street does not have is a user-friendly format for inputting investigative and intelligence information into his or her computer. Instead, the Agent faces a cumbersome, time-consuming process of preparing a paper record of that information, seeking the necessary approvals, then uploading the document into an existing database. If Agents had the VCF capabilities we envisioned, they could directly input information into their computers, receive electronic approvals, and, with the push of a button, upload information into the database where it would be immediately available to others who need access to it—Agents, analysts, other federal employees, and state and local officials.

I want to emphasize, however, that although VCF would enable us to do our jobs more efficiently, the absence of VCF does not prevent us from fulfilling our counterterrorism, intelligence and law enforcement missions. Again, VCF is not a

database or an analytical tool used to connect the dots—it is a case management system that will make it easier for Agents to input and share the dots.

Having said that, Mr. Chairman, I thank you for your longstanding interest in the VCF program and your commitment to hold a public hearing to examine the setbacks which have plagued this program. This afternoon, I would like to take the opportunity to answer three basic questions about VCF: (1) What went wrong? (2) Who is responsible for what went wrong? and (3) Where do we go from here?

What Went Wrong?

The development of the VCF application started with a very simple concept—the FBI's need for a modern case management system. As the FBI's mission evolved over the past several years, so did our technological needs. As a result of these changes and other issues, the FBI faced obstacles in a number of key areas relating to the VCF program.

—We did not have a complete set of defined VCF requirements when the original contract was signed in June 2001.

—The contract was based on hours worked—cost plus an award fee. We now know these types of contracts are difficult to manage. Although the requirements were solidified in November 2002, the contract remained a cost-plus-award-fee contract.

—We lacked skill sets in our personnel such as qualified software engineering, program management, and contract management. We also experienced a high turnover in Trilogy program managers and Chief Information Officers.

—We underestimated the complexity of interfacing with our legacy system, of addressing our security needs, and of establishing an enterprise architecture.

We will continue to confront these lessons moving forward.

Recognizing our internal limitations, we decided to outsource the development of VCF, including contract management and technology development. The contractor responsible for delivering the user applications component, including VCF, is the Science Applications International Corporation, or SAIC.

Following the establishment of solid requirements in November 2002, the original target date for completing VCF was December 2003. I personally received a demonstration of the VCF software in November 2003 and was impressed with what I saw. I believed that we were on the right track to deliver to our employees' desktops the case management system we were seeking. However, when SAIC delivered the product to us in December 2003, we immediately identified a number of deficiencies in VCF that made it unusable. Upon further examination, we discovered nearly 400 problems with the software and, in April 2004, provided SAIC with a document outlining the corrections needed. SAIC ultimately agreed to remedy the deficiencies and deliver full functionality but only at a cost—an additional $56 million—and a timetable—an additional year—which were unacceptable to the FBI.

In June 2004, I decided to adopt a new two-track plan for VCF: an Initial Operating Capability, or IOC, and a Full Operating Capability, or FOC. My goal with the IOC was to identify and utilize some portion of the product developed by SAIC, since the fully functional case management system had not been delivered. The portion of VCF currently being piloted in the IOC is the automated workflow process. Last month, several hundred employees in the New Orleans field office began using the system as their document routing system and will continue to do so through the end of March. The purpose of the pilot is to: test drive the workflow concept; validate the human/machine interface; create an electronic interface to our legacy system, the Automated Case Support System, or ACS; assess network performance; and develop and deliver an enterprise level training curriculum.

The IOC is on track to accomplish these objectives.

As part of Track Two, the FBI contracted with multiple independent vendors to perform the following tasks:

—Examine the VCF application delivered by SAIC in December 2003 to determine if the software as designed will meet the FBI's operational, security, and performance requirements. The contractor, Aerospace Corporation, was also tasked to determine if the VCF application is scalable and can be maintained and enhanced easily.

—Examine the current technologies and vendors, as well as available Commercial Off-The-Shelf, or COTS, software applications and those designed for other agencies, to determine the best combination to meet the FBI's needs. This effort was conducted jointly with the Department of Homeland Security to ensure our case management efforts would be interoperable. In many ways, the pace of technological innovation and the need for information sharing has overtaken our original vision for VCF and there are now products to suit our purposes that did not exist when Trilogy began.

—We have also asked a different contractor to review and revalidate our users' requirements because the mission of the FBI has evolved and there are new requirements for information and intelligence sharing among different entities.

Last week, we received the final version of the Aerospace report and provided copies to the Committee and to the Office of the Inspector General at the Department of Justice.

Who is Responsible for What Went Wrong?

Mr. Chairman, I am responsible, at least in part, for some of the setbacks experienced with Trilogy and VCF. I agree with the OIG's finding that "FBI management did not exercise adequate control over the Trilogy project and its evolution in the early years of the project." Let me also add that I agree with the OIG's finding that "with the new organizational structure and authority given to the CIO in July 2004, project management has been given the attention that was needed throughout the Trilogy project." Mr. Chairman, I will address that new structure and its accomplishments later in my statement.

In addition to our shortcomings in overseeing this project, however, the contractor responsible for VCF bears some responsibility. As discussed above, the FBI retained a not-for-profit, federally funded contractor, Aerospace Corporation, to conduct an independent verification and validation review of the VCF software as delivered by SAIC in December 2003. We asked Aerospace to provide responses to the following three questions:

—1. Did SAIC meet the stated requirements?

—2. Did SAIC develop a complete and correct Concept of Operations, System Architecture, and System Requirements?

—3. What should the FBI do with the VCF software as delivered in December 2003?

Aerospace concluded that "lack of effective engineering discipline has led to inadequate specification, design and development of VCF." In the course of their review, Aerospace could "find no assurance" that the requirements were satisfied, nor that the architecture, Concept of Operations, and requirements were correct and complete. Needless to say, Mr. Chairman, after three and a half years, this was disappointing news.

With regard to the funding of VCF, this Committee has been supportive of our efforts and has generously provided the funding we have needed to overcome obstacles and attempt to move forward. Mr. Chairman, you and the other members are undoubtedly concerned—as am I—about losses we have incurred, as well as future investments we will need to make, in VCF. We have invested approximately $170 million in VCF to date. It is my understanding our vendors have delivered services and reusable equipment worth $53.3 million and that we have $12.2 million in unspent obligations on our VCF contracts. This results in a loss of $104.5 million. I am disheartened by this result but remain confident in our ability to deliver a case management system to our employees' desktops in the future.

Where Do We Go from Here?

VCF

The development and deployment of an investigative case management system remains the top priority of the Office of the CIO. Some components of VCF that have been developed will be incorporated into the long-term solution. We will

—Leverage the permanent interface that has been established with our legacy data systems.

—Assess the impact of an automated workflow system on a field office and Headquarters structure, as well as the performance of a case management system on the new Trilogy network, during and at the end of the pilot testing; and,

—Take with us a number of valuable "lessons learned" in contract management, project management, policies and procedures, modular development and deployment, data security, and records management requirements.

Not surprisingly, the pace of technology has overtaken the development of unique software applications for the FBI, and we may turn to Commercial Off-The-Shelf, or COTS-based, products. We are currently reviewing the Aerospace reports which recommend that we discard VCF and start over with COTS-based products, and which provide their evaluation of COTS products as well as products in use by other government agencies. As we do so, we will continue to consult with industry leaders to ensure that we develop a sound, long-term plan for our IT needs.

We will move forward with a phased development and deployment plan as recommended by the National Academy of Sciences and required by Federal information resource management policy. An incremental approach ensures development and acquisition of the best available products on the market. Every phase will pro-

vide a set of services that the FBI workforce needs and which was part of the original VCF plan. I cannot at this time estimate when this will occur nor how much in additional funding we will need to invest to get there.

We will also give consideration to a Service Oriented Architecture (SOA), as recommended in the Aerospace report. The concept behind an SOA solution is to standardize enterprise services—such as searching, reporting, and analyzing data—so that different groups of users can reuse similar services to access dissimilar data sets throughout the enterprise—such as our legacy systems of ACS, III, and our Telephone Application. It appears that an SOA approach could provide a flexible solution to the inflexible systems currently existing within the FBI and would help us successfully implement a final product.

FBI Information Technology

With me today is Zal Azmi, who joined the FBI in November 2003 as the Chief Information Officer. Through his leadership, the FBI has implemented a coordinated, strategic approach to information technology.

—*Strategic Plan*.—In December 2004, we completed our first release of the Strategic IT Plan which maps out how IT will support the FBI's and DOJ's Strategic Plan and mission goals over the next five years. All IT projects are required to be consistent with the FBI's and DOJ's Strategic Plans.

—*Enterprise Architecture*.—We established our baseline Enterprise Architecture (EA) in 2004 and are in the process of developing our target EA. We have created an IT Master Systems List identifying all of the IT systems, applications, networks and databases in the FBI and DOJ. All IT projects in the future will be required to be consistent with the FBI's and DOJ's EA.

—*Process Improvement*.—Our Life Cycle Management Directive (LCMD), which governs how IT projects are managed from "cradle to grave," is now consistent with industry best practices and Federal government information resource management policies. All IT Projects and Programs are required to pass through rigorous project and executive level control "gate" reviews for each stage, from inception through disposal. There are 7 gates, 9 phases, and 14 key supporting processes in the LCMD. These reviews are the mechanisms for management control and direction, decision-making, coordination, and confirmation of successful performance.

—*Portfolio Management Program*.—This program focuses on performance assessments of IT investments in the operations and maintenance (O&M) phase of their life cycle. Since the majority of our IT investments currently reside in the O&M phase, these assessments help senior management make more informed decisions about IT investments, in terms of both personnel and money. Portfolio Management recommendations are focused on those investments that should be leveraged, replaced, outsourced or retired.

—*Enterprise IT Tool*.—The IT Portfolio Management Automation project awarded a contract to develop the FBI's Enterprise IT tool. This is a software package that will identify and track IT projects with baselined plans, schedules, and costs. It will also plan and track all FBI IT hardware and software infrastructure procurements at an integrated, enterprise level.

—*Capital Planning and Investment Management/Project Assurance*.—The Investment Management/Project Review Board now reviews and approves new IT investments at specified stages of each IT project's life cycle. We are also in the process of evaluating the FBI's 130+ existing IT projects for overall health and placement within the system development life cycle. This will enable FBI executives to uncover and address cost, schedule and performance risks. IT Investment Management will use our Enterprise IT Tool to track new FBI IT investments to ensure alignment with mission goals.

—*Performance and Results-Based Management (IT Metrics)*.—We are updating an IT Metrics program that identifies and measures IT performance according to industry standards, government regulations, and Earned Value Management System (EVMS) principles. Currently, we publish a CIO Monthly IT metrics report using the Balanced Scorecard Methodology. Our plan is to establish EVMS for "major" IT projects. When a program or project metric varies by more than 10 percent of the acceptable thresholds for cost, schedule, and performance, it will trigger closer scrutiny and remedial action by the Investment Management/Project Review Board.

—*Acquisition and Financial Reform*.—IT Acquisition Reform, a joint initiative between the CIO and the Chief Financial Officer of the FBI and DOJ, will standardize and automate all procurement actions, involving all IT acquisitions, as well as focus on increased competition and small business involvement. In 2004, the FBI entered into multi-year enterprise-wide agreements with Microsoft, Or-

acle and Dell which have saved millions of dollars in licensing fees. The savings derived from these contracts have been reinvested into technology projects, such as SIPRNET and FAMS (FBI Automated Messaging System). SIPRNET gives the FBI desktop connectivity to the Intelligence Community and FAMS is based on the Defense Messaging System (DMS). The FBI is the first civilian agency to operate a classified DMS-like system.

—*Leadership*.—We have begun to train our Program and Project Managers as well as executive management personnel to become certified as Program Management Professionals (PMP), which is in compliance with the federal guidance. We currently have two certified Government and five contractor PMPs. Approximately 25 managers have taken the PMP review course and plan to take the test. Another 20 are currently enrolling in the training program. This and other leadership training provides best practices and techniques to provide better management of the IT projects and the enterprise IT portfolio.

—*IT Policy*.—We are in the process of updating a Master IT Policy List. Once established, any new IT policies or modifications will have to be reviewed and approved by the IT Policy Review Board. The Master List will enable the CIO to monitor all IT projects during the Life Cycle Management Directive control gate review processes and enforce all applicable IT policies.

—*Technology Assessment*.—The FBI's Chief Technology Officer is working closely with the Enterprise Architecture team of the FBI and DOJ to standardize enterprise technology standards, technical reference models, technical architectures, and technical design reviews under the Life Cycle Management Directive and system testing/integration. A unified test and integration facility will allow for centralized technology assessment that provides responsive IT solutions to meet mission goals. These measures mitigate project risks through common, interoperable, supportable and affordable solutions.

—*Security and Information Assurance*.—We have implemented an Information Assurance Program which implements key IT capabilities such as Public Key Infrastructure (PKI) and the Enterprise Security Operations Center (ESOC), to strengthen IT services in the FBI and DOJ and mitigate internal and external threats. Certification and Accreditation is being required for all IT Projects and Systems to further mitigate project risk.

CONCLUSION

Mr. Chairman, in the aftermath of VCF, the FBI is faced with difficult decisions on how best to proceed with our evolving IT needs and evolving technologies. This Committee and the American people have my personal assurance that we will proceed as expeditiously and as prudently as possible to provide our employees with the automated capabilities they need. We have expanded the team of IT professionals within the FBI, each of whom has demonstrated an ability to perform under adverse circumstances. We have learned many valuable lessons over the past few years and, as a result, will be able to apply these lessons and avoid many of the pitfalls that befell this project in the past.

I would like to close by thanking the Committee, and you in particular, Mr. Chairman, for your support throughout this endeavor, and I look forward to working with you and your staff as we chart our course for the future.

Senator GREGG. The FBI has obviously got a problem and you are willing to address it and you have been forthright in explaining it, but I do think it is important to go back to some of the causes of the problem and make sure that those things are being addressed.

The Aerospace review, and I think choosing Aerospace, from what I can figure out, was a reasonable choice. They are independent and they appear to be quite objective. But they have three basic findings. One, that the 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. I want to get back to that point because I want to know if that was an intentional decision because it appears to have driven cost.

Second, the high-level documents, including the concept of operations, systems architecture, and systems requirement, were nei-

ther complete nor consistent and did not map to users' needs, which I find unusual.

And three, the requirements and design documentations were incomplete, imprecise, requirements in design tracing have gaps, and the software cannot be maintained without difficulty and is, therefore, unfit for reuse. We are looking at the 2003 delivery, of course, but this was the format on which 2004 was, I presume, built out of. And even if it wasn't, it still raises huge issues since we paid $170 million to get it.

And then Aerospace concluded that it would be better not to even develop it this way, that we should go to the off-the-shelf approach, which raises three fundamental issues which I am wondering how the FBI plans to approach them as it moves forward.

The first one is, why didn't we have in the FBI the technical people who would have picked up on things like failure of architectural design, failure to meet standards which were fairly consistent across the development of software architecture which weren't being met? There was a huge turnover of people during this period. Is it possible for an agency like the FBI to maintain the quality of people that are necessary in order to monitor a program of this size or should they—do we almost as a matter of systems have to put that monitoring into an independent group in order to make sure that we have the talent necessary to double-check a contractor like this?

Second, why would we ever choose a cost-plus contract? I mean, this experience of cost-plus is pretty horrific across Federal funding activities.

And third, this point which Aerospace makes about actually developing a software which wouldn't conform or wouldn't be integrated with off-the-shelf activity. We know by definition that technology mutates constantly and improves. I mean, isn't it inherent to any technological system of this size that you are going to want to be able to migrate to the next system, which is going to work better, and that next system isn't necessarily going to be internally developed, it is going to probably be developed by some smart bunch of folks who spun off from Massachusetts Institute of Technology (MIT) and are sitting in a garage somewhere in hopefully New Hampshire?

But it is not going to probably come from within the agency because you don't have the time and you don't have the people and you don't have the talent. Or you have the talent, maybe, but you don't have the time to focus on the mutation.

So have we addressed those three issues which I see as systemic to the question of why it has failed?

QUALITY OF PERSONNEL

Mr. MUELLER. Let me take a crack at them and then turn it over to Mr. Azmi.

In terms of the quality of personnel we had in the Bureau, I had a CIO, a very excellent CIO for the first year after I was there. He then retired. I then went on a nationwide search for a CIO which took about 8 to 12 months. The persons who were proffered for a variety of reasons fell through and there was a gap during that period of time in leadership at the CIO position. That hurt us.

I also, perhaps due to my naivete, did believe that we had the appropriate program managers. I had persons in from other organizations such as IBM and Lucent. I came to find out that there are project managers in a particular skill that we needed. I did not provide to our project managers or to the users group. It was a software engineer specialist with the capability of drilling down into that which was being composed by SAIC.

Now, do I have that capability now? I don't think, and I will ask Zal, I am not certain that we have that full capability to drill down into a particular software package and determine whether everything is going as it should go.

I do know that we have greatly expanded our CIO office under Zal Azmi. One of the things that he has brought is the ability to give me the bad news early on. One of the problems of anybody who runs an organization like mine is that people want to give you the good news. They do not want to give you the bad news. He has always been out there giving me the bad news and he has brought on board a technology officer who is the type of person that goes out and looks at each one of these COTS products.

All that being said, we will have to augment our staff with contractors. We will have to go and look, as we have in the past, for expertise outside the Bureau to make certain that we have covered all of these areas of expertise.

COST-PLUS CONTRACT AND COTS PRODUCTS

As to your second question, on a cost-plus contract, that was entered into in the summer of 2000. I do not have the facts or the understanding as to why we entered into a cost-plus contract in the summer of 2000, in the summer of 2001. I can tell you that my experience is we will never again in the Bureau enter into a cost-plus product that can lead us so far astray.

I will tell you that prior to the last piece of the second part of Trilogy, which was putting in the networks, the local area networks, the wide area networks, at the secret level, at the classified level, which was a challenge, we had difficulties with the cost-plus contract with that contractor and ended up restructuring it so we got a commitment to produce at a particular cost at a particular time.

Last, with regard to COTS products, as I become more knowledgeable about technology, it goes without saying, I think, that the world has come to be a plug-and-play world. You don't get a full system of stereo television all in one package by one manufacturer now. What you have is plug and play, whether it be computers or your stereo or what have you. As we have grown since 2001, it is clear that in developing a package such as the Virtual Case File, we have to look at COTS products. We have to use COTS products. We have to phase it in, understanding that down the road 1, 2, or 3 years hence, we may have to unplug a product and plug in a new one.

Zal, do you have anything to add?

Mr. AZMI. I want to add to the concept of cost-plus contract. The Bureau originally actually got into this contract in 2001 because we did not have all of our requirements defined. However, in 2002, there was a joint application development session between the Bu-

reau and SAIC and, at that point, we developed a solid base for requirements, and, at that point, that contract could have gone to a performance-based contracting. However, that contract continued as a cost-plus contract.

I will say that in June 2004, when we decided to actually develop the initial operating capability, we did move to a performance-based contract. That is the main reason why the software was developed on time and within the budget.

I would also add that even though IOC is only 10 percent of the VCF, I think the concept is sound and we can implement that for larger contracts.

ENTERPRISE ARCHITECTURE

The other question, Mr. Chairman, you had was about enterprise architecture and what we are doing, where we are going from here. I submit to you that we have already solidified our requirements for Virtual Case File or a case management system of the future. We have already mapped those requirements through a Federal enterprise architecture framework, which is the best practice, is the standard the Federal Government uses. We have already mapped our software, or our requirements to what they call a service reference model. We have already done this mapping.

That will enable us to actually deliver a case management system of the future in phases, with capabilities being available to the users shortly after the contract is awarded, and that is the concept we are going to move forward with, the small deliverables and the contained time with program management and project management disciplines in place.

HOW DO WE GET THE MONEY BACK

Senator GREGG. I want to make sure everybody has time here so I will reserve my questions, but I am sure somebody is going to ask you how we are going to get any of this money back and that is a question I do hope we get to.

DELIVERY ELEMENTS OF VCF ON TRACK

Senator LEAHY. Thank you, Mr. Chairman, and I would ask also consent that I have a little time to put my full statement in the record and keep this short.

Senator GREGG. Of course.

Senator LEAHY. The reason I ask is that it would be somewhat more lengthy because it also involves my other hat on authorization.

Director Mueller, on May 20, 2004, you testified before the Judiciary Committee. You stated, "We are on track to deliver elements of Virtual Case File capabilities by the end of this year." I responded to that and I said, "What elements and what do you mean by elements?" I don't think I ever got a clear answer on elements, but you did say, quote, "We are in negotiations with our contractor on finishing out that last part of the Trilogy project, the Virtual Case File, and my hope and expectation is that that will be completed by the end of this year. But I do believe that when we are

concluded this year"—2004—"we have the foundation for cutting-edge technology for an organization our size," close quote.

At the same hearing in May 2004, Senator DeWine of Ohio asked you this. Quote, "Do you currently have enough money to complete Trilogy? What will be the total cost of Trilogy? How much money do you have left to spend on the program, and when will Trilogy be completed?" You responded, "I believe we do have sufficient money. I believe the total cost will be close to $560 million. And the last piece of Trilogy, that is the Virtual Case File, my expectation, it will be in by the end of this year." Senator DeWine said, "End of this year?" You responded, "This year."

Now, we do know that by the time you testified in May 2004, almost 1 year ago, Virtual Case File was already on life support. The FBI had already twice rejected SAIC's delivery of the Virtual Case File. It already identified nearly 400 potential problems with the software. It had already been told by Virtual Case File that correcting these problems would cost an additional $56 million and an additional year. As you say in your testimony today, they are both unacceptable to the FBI.

In addition, the FBI was already negotiating for a scaled-down version of VCF, the initial operating capability of VCF Light.

Just the day before the hearing when we asked you these questions where we got a pretty rosy scenario, the FBI submitted a request, Federal Systems Integration and Management (FEDSIM), the contract manager, to estimate the cost associated with shutting down 90 percent of it.

Now, I don't know anybody who has been more supportive in the 30 years I have been here of the FBI than I have. Others have been as supportive. I don't know of anybody more supportive. I have been extremely supportive of you. But I am ready to tear out what little bit of hair I have left.

Why didn't you mention any of these problems, all of which were there, when you were asked about the status of the project in May 2004? You had a friendly audience. You had me. You had one of the leading Republicans, Mike DeWine. We were asking you these questions, and the answers we got didn't comport with the facts. Why?

DIRECTOR MUELLER'S RESPONSES

Mr. MUELLER. Senator, I don't want you to lose the last of that hair.

Senator LEAHY. There is not much left, I can tell you right now, nor is there any more patience.

Mr. MUELLER. I will tell you, as we went through the spring—and I would have to look at the dates—as we went through the spring last year, I had voices telling me, particularly from SAIC, that they could produce. I met with the Chief Executive Officer (CEO) in the spring—I am not certain of the date—and received from the CEO the assurances that we could—and by "we," I mean SAIC would produce and it was my expectation that we would have a substantial portion, not all, but a substantial portion of Virtual Case File by the end of the year.

Now, when that came in terms of the timing of my testimony, I am not certain. On the other hand, I will tell you that Zal Azmi

has always raised questions about this. I knew that there were issues with regard to the project as it was given to us in December 2003, but I had already been through a similar circumstance with Computer Sciences Corporation (CSC) in which we had to renegotiate, we had to go back to the drawing table, and they came through under budget, on time, as we had done so. And there was a part of me in the spring of 2004 that thought that we could go through exactly the same exercise.

FEDERAL SYSTEMS INTEGRATION AND MANAGEMENT REQUEST

Senator LEAHY. The day before the hearing, the FBI had submitted a request to FEDSIM asking, what would it cost to shut down 90 percent of it.

Mr. MUELLER. I am not familiar with that. I am not certain I was familiar with that at the time.

Senator LEAHY. I hope not, because if you were familiar with it, your answers to mine and Senator DeWine's questions were totally inconsistent with what the facts were.

And then we sent follow-up questions to you. I did and several others did. You told me you completed your responses some time ago and sent them on to the Department of Justice for review. It has been 8 months. I don't know who is good cop/bad cop, to use an analogy in your business, who is good cop/bad cop here, but we asked specific questions. The answers we were given did not comport with the facts, and I will accept your statement here today that you were not aware that the day before, they were trying to figure out how to close down 90 percent of it.

But the answers—somebody has got to bear responsibility. It can't just simply be, well, the Department of Justice told us for 8 months, don't answer these questions. We are talking about hundreds of millions of dollars and a friendly committee. What in the hell goes on if it is an unfriendly committee?

Mr. MUELLER. Is that a question, Senator?

Senator LEAHY. Yes. When are we going to get the answers?

Mr. MUELLER. Well, as I indicated to you yesterday, the answers were provided to the Department of Justice in October. We have been working with them. I am as frustrated that you do not have the answers as you quite obviously are and I am certainly willing to do what I can to work to get those answers to you.

BUDGET TO COMPLETE TRILOGY

Senator LEAHY. Well, let me ask you a specific question for appropriations. Does the FBI have sufficient money to complete Trilogy, including VCF or a similar case management system, or will the FBI reprogram or request additional funds to fix and find a replacement for Virtual Case File in this upcoming budget cycle?

Mr. MUELLER. What we are planning to do is utilize funds that we have outstanding for this fiscal year and in 6 to 8—and correct me if I am wrong, Zal, on this—and in 6 to 8 weeks, we ought to have a better feel for what it would cost to bring on the various components that we are anticipating bringing on in the phased-in development of Virtual Case File. It would not be a 1-year phase-in. It would be a 2- or a 3-year phase-in. At this point in time, having just received the Aerospace report, we are examining all of our

options and it will be at least 6 to 8 weeks before we can come back to you and lay out in front of you our strategy and say, this is what we want to do. These are the COTS products we may want to use and this is what it will cost.

I am looking to reprogram funds to do it, certainly within this fiscal year, and then we will look at where we are when it comes to 2006–2007.

REPROGRAMMING

Senator LEAHY. Well, if you reprogram the funds——

Senator GREGG. Senator, if I can just interrupt, I think it is important to note this phased-in development issue, because this committee was actually very aggressive with the FBI saying that this program should have been phased in at the beginning——

Senator LEAHY. I remember that.

Senator GREGG [continuing]. As I think the Director will recall, and so I think at least they should be credited with the next steps they are going to do phases.

Senator LEAHY. But then on that, where are you going to reprogram the money? Does that mean you are going to reduce other programs?

Mr. MUELLER. We have carryover money of approximately $15 million and we are looking at other savings that we have managed to put into Virtual Case File, or what will become Virtual Case File, and we are also going to look at reprogramming additional funds, depending on what we can do and how fast we can do it in this fiscal year.

Senator LEAHY. Will you report to this subcommittee—well, the reprogramming, you will anyway——

Mr. MUELLER. Absolutely.

Senator LEAHY [continuing]. But will you report to this subcommittee from what programs you are finding savings?

Mr. MUELLER. Yes.

Senator LEAHY. You understand the danger of that, of course.

Mr. MUELLER. Yes.

Senator LEAHY. All right.

Mr. MUELLER. I would anticipate we would have to. We reprogram—if it is over a certain amount, we are up here in any event, so——

Senator LEAHY. We are just curious——

Mr. MUELLER [continuing]. It is an ongoing——

RECOUPING FUNDS FROM SAIC

Senator LEAHY. We are just curious what programs that we have already authorized might get cut back or eliminated by a reprogramming to take care of the mistakes in the VCF. By the way, speaking of money, do you have plans to recoup funds from SAIC, and if so, how much?

Mr. MUELLER. We have referred the matter over to the Department of Justice to look at, explore our options.

Senator LEAHY. Are they going to get an answer back to you quicker than they do to those of us in the Congress?

Mr. MUELLER. All I can tell you is we referred it to the Department of Justice, Senator, looking at to what extent either of the

parties are culpable. I do believe there is culpability, as I indicated, on both sides. I am not going to stand here and say that we are not in some part responsible for the fact that it was not brought home on time. But as I say, I believe SAIC was also responsible. The report from Aerospace seems to indicate some of those deficiencies and we are looking at our options to recover some of that money for the taxpayer.

Senator LEAHY. Do you have any estimate of how much that might be?

Mr. MUELLER. I do not.

CASE MANAGEMENT

Senator LEAHY. Okay. Let me ask you just two questions and I will submit the rest, which is always scary because I will probably never get the answer, but when will agents have a functioning case management system in their hands?

Mr. MUELLER. A basic case management system, and there are various aspects to it—monitoring evidence, leads management, and the like, but a basic case management system, certainly we hope within 1 year. And I will tell you, I am guilty of——

Senator LEAHY. One year from today?

Mr. MUELLER. Yes. And I am guilty in the past of raised expectations. I thought we were going to produce. Every time I have gone to an office to talk to our people, I will talk about the importance of technology, the desirability of bringing us into the digital age, and have given them the expectation that we would have had Virtual Case File certainly by now. I went out and retrained a number of agents in support of Virtual Case File. So I am very reluctant to give estimates, understanding that I have been proven wrong in the past and I have raised expectations, not only of the agents but also of Congress and others who are interested in moving us into the digital age.

INFORMATION TECHNOLOGY DEVELOPMENT AND FUNDS RECOVERY

Senator LEAHY. I will ask just one last question and I will submit the rest, and I ask this question because the same frustration—the biggest frustration I have in being unable to get answers is that over and over again on the things that we legitimately ask questions about, either the Appropriations Committee or the authorizing committee, we don't find out until we read it in the paper. We either find out because a newspaper reporter is able to get more or a TV reporter, or somebody has leaked something to them.

So let me ask you this. Are there other clouds on the horizon with respect to the information technology efforts that you might like to tell us about today before we read about it in the press in the future?

Mr. MUELLER. That is a very broad question.

Senator LEAHY. I know it. It is a very broad subject.

Mr. MUELLER. Are there any clouds on the horizon with regard to the development of these systems? With regard to the development of these systems, I think the last piece of Trilogy was Virtual Case File, and I think you know exactly what we know with the various reports. We, upon occasion, have other areas in which technology is affected. We are currently looking at an issue that does

not relate at all to our sensitive material—well, our classified materials, but is an issue which I probably should raise to you in private.

Senator LEAHY. Okay. Fair enough. Will you?

Mr. MUELLER. I will.

Senator LEAHY. Thank you. Thank you, Mr. Chairman.

Senator GREGG. Senator Mikulski.

Senator MIKULSKI. Thank you very much, Mr. Chairman.

Well, under this rock is another rock and under this rock is a black hole. The future—I am concerned. First of all, we can look back, but my concern is how do we move ahead.

Can you tell me, number one, are you thinking about scrapping the program now that we have invested $170 million into it, or how much of the $170 million are we able to kind of recapture and get value for the agents to have what they need in the field? Are we just bagging it? We have got so many contractors there. You have got SAIC, and others working on the other parts of Trilogy and of course now you have Aerospace, the corporation's comments and evaluations. Where are we here? What are you going to do? Are we scrapping a $170 million program here?

Mr. MUELLER. Let me start, Senator, by saying that the total contract was for $170 million. We think we can recover approximately $53 million of that in terms of software, hardware that we have received in the course of that contract, so that will not be lost. We have in excess of $12 million left in the contract, which leaves approximately $104 to $105 million that we will not be able to recover.

POSSIBILITY OF SCRAPING SAIC

Senator MIKULSKI. Are you saying goodbye to SAIC now or are they going to be the ones that everybody walks into the woodshed, but then what happens after you come back from the woodshed to the main building? Are we going to get the case file——

Mr. MUELLER. We are looking at all of our options and who can——

Senator MIKULSKI. So you don't know who——

Mr. MUELLER. We do not know who the contractor will be for the next phases of the program. Now, are we scrapping the program altogether, I think was one of your questions.

Senator MIKULSKI. Yes.

Mr. MUELLER. The recommendation from Aerospace, based on their review of that which was provided to us by SAIC in December 2003, was to scrap the project totally. We are looking at that. We are reviewing that. SAIC, I think, will tell you when they testify that the product that they have produced for us that is being tested down in New Orleans is state of the art. It is very good and we should adopt that. We are looking at that.

On the one hand, SAIC says we have produced and the product we have got down in New Orleans is good and you ought to adopt that. On the other hand, we have the report from Aerospace that says, for a variety of reasons, you ought to scrap Virtual Case File. So we are evaluating those two——

Senator MIKULSKI. But SAIC says, we have delivered you an initial product. It is now in New Orleans being tested.

Mr. MUELLER. Yes, and it is good, state of the art——

Senator MIKULSKI. Well, wait. Wait. We don't know yet. It is being tested.

Mr. MUELLER. That is what SAIC is saying.

Senator MIKULSKI. It is being tested.

Mr. MUELLER. It is being tested.

Senator MIKULSKI. So, number one, you don't know whether you are going to scrap it or not, and if you do, whether you scrap it or not, moving ahead, you don't know who the contractor will be. And if you don't know who the contractor will be, then you don't know how much it will cost——

Mr. MUELLER. Correct.

DECISIONMAKING

Senator MIKULSKI. So this is not a happy situation.

Mr. MUELLER. No. I would agree with that. It is not a happy situation when we are——

Senator MIKULSKI. And then my question becomes, then, who is in charge to get this back on track and what are your time tables? The chairman will have an appropriations deadline. We have a very tight budget—we have been faced with spartan allocations. And then who is going to be in charge to make all these decisions? And I know you are going to say you are in charge, okay. That is great. But like the Pope is in charge of the Catholic Church, who is in charge of this confessional?

Mr. MUELLER. Well, the way you put it, maybe I am in charge of the confessional, but I will rely on Zal Azmi and his team for advice and management of the process as we go forward. But as I said before and I have said since I have arrived, and I have said it in this context and other contexts, we need and would look to outside, independent advice on whether we are on the right track. We have had—and I have gone to any number of outside entities to get advice on whether we are on the right track, experts outside, and we will continue to do that.

Senator GREGG. Senator——

Senator MIKULSKI. Well, my time is up——

Senator GREGG. No, your time is not up, but I am just wondering if I could interject a question here.

Senator MIKULSKI. Please, yes. I think this will work best this way.

EVALUATING THE 2004 PRODUCT

Senator GREGG. Are you evaluating the 2004 product as it is now being used in a demonstration in New Orleans independently, and if you are, who is doing that?

Mr. AZMI. That product in New Orleans is a prototype or a functional prototype of the VCF IOC, initial operating capability. That software is one-third of the—I am sorry, one-tenth of the VCF software. It is not all of the capabilities that was promised. It is just one-tenth of that. Within that software, the FBI has also included a number of capabilities that were developed by FBI staff, programmers. So, that is a combination of two programs that is being tested in New Orleans.

By the end of March, we will shut down that evaluation period and will have 30 days to actually gather information and feedback from our users in New Orleans to see how they liked it. That is the work we are doing with our staff over in New Orleans, sir.

Senator GREGG. Can I postpone you for one more question?

Senator MIKULSKI. Sure.

Senator GREGG. You are saying it is one-tenth of what was supposed to be delivered.

Mr. AZMI. That is correct, sir.

Senator GREGG. The project that was evaluated and found so lacking by Aerospace, which was the 2003 product, was that the entire product?

Mr. AZMI. That is correct, sir.

Senator GREGG. Thank you.

Mr. MUELLER. I think——

Senator MIKULSKI. Did you want to pick up on my question?

Mr. MUELLER. I think Mr. Azmi wanted to add on the answer to your question, if he could.

Senator MIKULSKI. Yes.

Mr. AZMI. I know that Director Mueller is taking responsibility for the program as a whole, but as the Chief Information Officer for the FBI, it is my responsibility to develop information technology to our users. What steps have I taken since my arrival to actually make sure——

Senator MIKULSKI. When did you arrive?

Mr. AZMI. November 2003, ma'am.

Senator MIKULSKI. Thank you.

Mr. AZMI. We have taken a number of steps to actually correct the deficiencies overall with information technology programs within the FBI. But specifically for the VCF program, what we have done, we have completed our requirements. We have a requirements document for a case management system that our users, our agents, and our analysts want and the FBI. We have mapped those requirements toward services that are guidelines by the Federal enterprise architecture framework. We have those services. We have broken down those services into phases to ensure that we have the ability and capability to deliver those into phases.

We have also asked another independent contractor to develop what we call an independent Government cost estimate to tell us exactly how much every one of these phases will cost. That report is due to the FBI by mid-February, ma'am.

Senator MIKULSKI. I appreciate that answer. I know my time is about up——

Senator GREGG. You have as much time as you want.

Senator MIKULSKI. Director Mueller, did you——

Mr. MUELLER. I wanted to add one other thing that has become important. It was in the National Sciences report, and that is the necessity for an enterprise architecture for the FBI as a whole. We have never had an enterprise architecture. We have been stovepiped. And one of the things we have done over the last year is begin to develop an enterprise architecture so that whenever we bring on an information technology product, it fits within that enterprise architecture.

For us to move forward, we have to have the enterprise architecture to assure that whatever we bring in is consistent with and works with other software and hardware packages that we may bring on board, and that is a substantial advance for us. We have a team working on it and I think we are on the track to have one of the better enterprise architectures for any institution in Washington.

ACCELERATED FUNDING AND OVERSIGHT

Senator MIKULSKI. Well, I appreciate these answers and I certainly your attempt, Mr. Azmi, to try to bring order out of chaos. I also appreciate the fact that after September 11, there was this incredible need to retool the FBI. There was an accelerated ops tempo, if you will, because we didn't know when they were going to try to kill us again. We were still standing sentry because they might be trying to kill us again in an hour and a half.

So we understand the challenges you faced, the FBI faced, and with this increased ops tempo, though, your Congress gave you money as well as in a variety of homeland security agencies money to protect the United States of America. That is what these files and all this technology is all about, is to maximize and leverage an agent to make that agent the most effective person that they can to do the mission.

I am really concerned that after 3½ years, where in the hell are we and have we just wasted money, have we just wasted time, and how we won't repeat it again, because in the report, it talked about how the FBI had changing requirements. It is what we hear at the Pentagon. Every time they build a ship, they meet with an admiral and a boatswain's mate and the requirements get changed.

So my question—well, first of all, just know, I know you are disappointed and I am disappointed. I believe that this is a systemic issue with some of the accelerated funding in homeland security and I think calls for additional oversight in appropriations.

But now having then come back to where we are, with the reforms Mr. Azmi has put in to bring order out of chaos, when do you think you can tell the subcommittee what it is that you want to do and how much it will cost?

Mr. MUELLER. Two months.

Senator MIKULSKI. Two months.

Mr. MUELLER. I think we will have a much better handle on where we are at that time.

Senator MIKULSKI. Fine. But I think we also have to understand the pressure that you—when I say you personally, because we were together in some tough environments and I respect you very much and all the agents. But, wow, I think we kind of have to regroup, don't you agree, Mr. Chairman?

Senator GREGG. As usual, the Senator from Maryland has gotten to the essence of the issue.

Senator MIKULSKI. Thank you. We look forward to working with you, Mr. Chairman, and we look forward to making sure there is not an empty chair here.

INDEPENDENT EVALUATING ASSISTIVE TEAM

Senator GREGG. It would be very enjoyable were you in that chair.

And just to follow up on the Senator from Maryland's points, which I think are absolutely correct, and Senator Stevens actually made this point before he had to leave, this could be a systemic issue across other agencies, as we tooled up so quickly with technology that agencies that didn't have the personnel capability to properly manage this tooling up either bring online technology that can't migrate into the greater needs, can't keep up with the changing times, or simply can't do the job.

That is why I get back to this issue of should we have an independent evaluating assistive team, where we have the level of expertise there that is consistent and technically current to come in and help an agency like the FBI. I mean, you have got a good person in Mr. Azmi. I am extremely impressed with Mr. Azmi. I have had a fair number of discussions with him. But is the FBI ever capable of getting out of the trees and looking at the forest on the issue of technology the way an independent group might be able to help you?

Mr. MUELLER. I think it is worth exploring. I think, as I have come to learn, that development of software for a particular organization requires a complement of individuals within the organization who understand the work of that organization——

Senator GREGG. That is obvious.

Mr. MUELLER [continuing]. Usually called user groups, and the experts on the other side who know the technology. And the coming together of those two is exceptionally difficult. A third party with the expertise, or a third entity that could provide the expertise to an agency may be worthwhile.

Right now, we understand we don't have all the areas of expertise in the Bureau and we go out to outside contractors to bring that expertise in, in particular areas. But it is certainly something that perhaps should be explored.

I will tell you also, in response to Senator Mikulski's point about pushing hard on the technology, one of the things that we did do which I think backfired on us is push hard after September 11 to get the technology on as fast as possible without understanding, fully understanding the detrimental side effects to pushing too hard to get that technology on board without going through, unfortunately, some tedious, time consuming steps in order to get what you need, even though you have to delay, and that is a lesson I have learned in the course of working with Virtual Case File.

FILE MANAGEMENT AND WIRELESS TECHNOLOGY

Senator MIKULSKI. Mr. Chairman, just to you, after 9/11 and then for those of us on the Intelligence Committee also authorizing and appropriating with the FBI, it was, in every one of the agencies where there was responsibility for protecting us against predatory attacks, there was this increased tempo and every desire to move quickly, even if we made mistakes. It was better to make a mistake and spend the money, but don't dilly-dally on the process.

At the same time, we had that sniper in Maryland, and I wish you could have been there to see the FBI, Bureau of Alcohol, Tobacco and Firearms (BATF), hundreds of agents in a room about this size with wireless technology. That is when I got a sense of the files, the management, and the communication, how they all worked with all of the leads all over America, with BATF and the ballistic lab, and then local law enforcement. It was really stunning. And when we have the right tools, it is amazing. But again, they were at the edge of their chair, working with every tool at their disposal, and even though some of those tools were out of date.

So again, we see the way they have to escalate to an intense level. They have an attitude which we appreciate. Damn the torpedoes. So if you make mistakes or you spend too much money or whatever, at least grab the sniper, grab the killer, grab the terrorist, grab the predator, and we have made mistakes. These are big-bucket mistakes, but now it is to regroup.

But I think it wasn't because there wasn't a desire to move quickly and do a good job. I am not white-washing this, but——

Mr. MUELLER. If I could respond briefly, Mr. Chairman, I think if you look at it as a continuum, after September 11, if you went into that room, you saw paper all around——

Senator MIKULSKI. You did.

Mr. MUELLER [continuing]. Because we would have to take down everything on paper and run it by paper. And if you went into our SIOC in the wake of September 11, you would find piles of paper around.

We evolved. When we worked with the other agencies, Federal and local, it was pretty much a paperless organization, and we have evolved to be paperless when we have challenges such as that.

Unfortunately, we had to run files between offices. We did not have the communications capabilities at the time of the sniper attacks that we would want, even though we had the paperless entry of information, and we have evolved yet from there.

So we have made headway in a number of these areas that enables us, particularly with substantial challenges such as September 11 or the sniper attacks and the like, to do our business digitally.

CLOSING REMARKS

Senator GREGG. Thank you Senator, which I think gets back to what our purpose here is, is to make the agent on the street more effective in protecting us. We know the commitment of the Bureau. We know it is extraordinary. We know the people that serve us there, including right up to yourself, are the best and trying hardest and we respect that, but obviously the taxpayers want to make sure they get value for their dollar, as you do, too. So that is what this hearing is about.

I thank you. Thank you for your time. I appreciate your courtesy in giving us so much of your time.

Mr. MUELLER. Thank you, Mr. Chairman.

Senator GREGG. Thank you, Mr. Director, Mr. Azmi.

SUBMITTED STATEMENTS

We have a bit of an issue here in that we have got a vote at 3:30 and a 4 o'clock event that I have to be at because the leader told me I have to be there and I am a big fan of the leader. So I think I am going to have to recess this hearing and probably reschedule the second panel, which I regret, because I think SAIC has every right to make their case in the public. They have obviously got a case they want to make as to their views, and obviously we would like to hear from Aerospace and from the Inspector General.

The statements from these organizations not appearing and a statement from Senator Grassley will be inserted in the record.

[The statements follow:]

PREPARED STATEMENT OF ARNOLD L. PUNARO, EXECUTIVE VICE PRESIDENT, SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

Chairman Gregg and Senator Leahy: It is a privilege to appear before you today to testify concerning our portion of the work on the Trilogy Project for the Federal Bureau of Investigation. Mr. Chairman, I ask consent that my entire statement be entered into the record and with your permission I am prepared to summarize.

INTRODUCTION AND CONTEXT

At the outset, let us say clearly that SAIC understands and appreciates the overwhelming demands and difficulties that the FBI has faced since the attacks of September, 11. While we disagree with the Bureau over aspects of the Trilogy program history, we have only the greatest respect for the dedication with which the Bureau has pursued its mission of defending our nation under the enormous, and sometimes conflicting, pressures that surfaced in the aftermath of the terrorist attacks.

SAIC, with 45,000 employees, is the largest privately owned research and engineering firm and one of the largest government contactors in the nation. As employee owners, we have prided ourselves since our founding 36 years ago on our ability to assist the U.S. Government on programs of national importance. Our dedication to work that matters is further reflected in an aggressive and pervasive ethics program. How our company operates and how we are perceived are matters of vital, personal interest to each and every employee. We have grown to become a very successful and sought after company by providing quality products and creating satisfied customers.

In that respect, let me mention several major, illustrative software engineering projects successfully designed and deployed for the FBI to illustrate the work we've done.

—The Combined DNA Index System (CODIS) is a national DNA database system for use by United States and international law enforcement authorities by creating DNA profiles and by matching unknown profiles found in the course of criminal investigations to profiles stored in local, state, and national databases here and overseas.

—The FBI Interstate Identification Index (Triple-I) is the U.S. national criminal history system that maintains more than 40 million data entries (the largest and most accurate criminal history database in the world) and is used every day by state, local and federal law enforcement agency in the United States.

—The National Instant Criminal Background Check System (NICS) implements the Brady Act. SAIC was contracted to develop, deploy, maintain, and support the federal, state, and local governments in checking a citizen's eligibility to purchase a firearm (handing in excess of 30 million purchases to date). It handled more than four million calls per year from firearms dealers checking purchasers against the national database. To quote Mr. Michael D. Kirkpatrick (FBI Assistant Director in Charge, Criminal Justice Information Services Division at the time of the work) in his letter of appreciation to SAIC in January 2004, "Not only is the successful implementation of the NICS directly attributed to the hard work and dedication of the SAIC staff, numerous post-implementation challenges were met head-on and overcome with SAIC's support—you have been a trustworthy, customer-oriented partner."

—Law-Enforcement Online (LEO) is a 24 hours a day, 7 days a week, online, real-time, controlled-access web portal (more than 43,000 users) providing a focal

point for electronic communication, education, and information sharing for the law-enforcement, criminal-justice, and public-safety communities nationwide.

In sum, SAIC comes to this issue with a record of outstanding achievement in challenging projects, including specifically for the Federal Bureau of Investigation. We point this out not to boast, but to provide the context for considering some of the issues that have marked the public discussion of Trilogy and the manner in which SAIC has performed on this contract.

The Results and the Reasons

—Trilogy began in a pre-9/11 world with very different circumstances and requirements than those that exist now.

—The events of 9/11 caused massive and continuing change in the project while the FBI dealt with enormous post-attack pressures and demands.

—The FBI's requirements for the project—the list of what the FBI wanted the project to have and do—grew and changed continually while turbulence in FBI program management worked against stability and definitive guidance.

—A key FBI decision to drop a controversial, high-risk plan for a one-step conversion to a new system opened the way for a sensible developmental approach of incremental improvements in capability.

—The FBI and SAIC renegotiated the contract in summer 2004, coming to firm agreement on requirements for the incremental improvement through what is called the Virtual Case File (VCF) Initial Operating Capability (IOC).

—SAIC acknowledges some areas where we made mistakes and particularly where we failed to adequately communicate our concerns to appropriate levels of management, to include the Director of the FBI.

—SAIC delivered, and the FBI approved and accepted, VCF IOC within the allocated budget and ahead of schedule to industry-standard quality, offering FBI agents significant new tools in their counter-crime and counter-terror roles.

Currently, the contract has a negotiated value of $130.3 million and a funded value of $123 million. To date, SAIC has been paid $115.2 million. We expect to be paid the funded value of $123 million at completion. In conjunction with this work effort, the company has invested $3.9 million of its own money to support the Trilogy program.

Aerospace Corporation

Before presenting SAIC's testimony about the course of its work on Trilogy in detail, I want to speak briefly to the report by the Aerospace Corporation. While we have not been given a copy of this report, we were allowed to read a copy last week at the FBI. We appreciate that opportunity. Aerospace Corporation did not inform us, nor attempt to discuss in any way its findings—a lapse we find both inexplicable and contrary to the practices of inspectors general, the General Accounting Office, and other scientific groups, who find that comments from those reviewed contribute to a more balanced and useful report.

The Aerospace Corporation produced a report on the wrong software while failing to concentrate on central issues that determine system performance.

Had they asked us for comment, we could have told them they examined the wrong software. Mr. Chairman, I mean that in a literal sense. Aerospace Corporation explicitly evaluated a snapshot in time of the software as if it were a finished product when in reality, as everyone should have known, it was still being developed. The Aerospace Corporation says it found "evidence of incompleteness" and "failure to optimize." This is hardly unexpected in a work in progress that was still months away from its delivery date. In academic terms, it was as if we had been assigned a paper due December but then graded it the previous summer.

The product we presented to the FBI in December 2004 is not the product evaluated by Aerospace Corporation. VCF IOC was rigorously tested and accepted by the FBI after meeting 100 percent of its requirements.

Because the software evaluated was different from the software delivered, SAIC believes that the Aerospace Corporation report is not an adequate basis for deciding on a future course of action concerning VCF.

This is not to say we accept Aerospace Corporation's judgments about the product that was evaluated. We emphatically do not. The Aerospace Corporation is a national asset in its realm of expertise: aerospace. The Trilogy project is something else, altogether. We respectfully—but strongly—urge this subcommittee to consider that Aerospace Corporation did not bring a sufficient understanding of the uniqueness, complexity, and scope of the FBI undertaking to evaluate our software product.

Central to the Aerospace report is criticism of requirements documentation. Time and again, in the Aerospace report we reviewed, we saw instances where criticisms

about requirements were based not on the substance of the requirements or whether or not the product satisfied the requirements, but rather on ancillary data such as syntax in documentation. How well the product satisfied requirements was not a part of their evaluation. Based on examination of the documentation they concluded they were not assured the product would meet requirements and went no farther.

In particular, SAIC categorically rejects the assertion that its work lacked engineering discipline, an assertion that appears without support in the document we read. This kind of assertion, without rigorous—or even specific—support should be unacceptable in an endeavor of this importance. For instance, Aerospace Corporation did not look at the software development folders, which are key documents on how the code was designed and written. These comprise the "Bible" for software developers. In a football analogy, it was as if Aerospace Corporation was asked to scout another team which had made available its playbook. They didn't bother to read it. In fact, they scouted the wrong team.

Even so, Mr. Chairman, we would welcome the opportunity, late though it may be, to discuss the findings with Aerospace Corporation. It could only benefit the FBI, which is our aim here.

SAIC'S PARTICIPATION IN TRILOGY

The FBI's Trilogy program is a massive, multi-part, multi-contractor program for broad-based modernization and improvement of its information technology. In June 2001, SAIC was competitively awarded a cost-plus-award fee developmental contract for the Trilogy User Application Component (UAC). This is an appropriate contract type because the project involved first working with the customer to develop and agree on what was needed (the requirements) and then execute the agreed tasks. The complexity and uniqueness of the missions of the Bureau also argued for this approach. Some of the public discussion of the Trilogy contract has been conducted as if the required tasks were well known at the start, and easily achievable. At no point in time has either condition existed.

At the time of award in June 2001, the contract scope for SAIC called for development of a web front-end to the existing legacy applications used to manage case information. When this effort was complete, SAIC was to define an Enterprise Case Management System. This was a measured low-risk approach building on existing, or legacy, systems within the Bureau.

The attack of 9/11

The September 11, 2001, attacks had as profound an affect on this project as it did elsewhere in the nation. Following 9/11, the Bureau faced enormous and sometimes conflicting pressures. Prior to the attack, the Bureau was dealing with revelations that a spy, Robert Hansen, had plundered FBI secrets. Security and integrity of information is a fundamental issue for the FBI. After the attack, it faced three often conflicting demands:

—The need to share information in the post-9/11 world so authorized personnel could both see and connect the dots to analyze and exploit intelligence.

—The need, in the post-Hansen world, to prevent all but a few specifically authorized people from seeing truly sensitive information.

—The need to ensure admissibility of investigative information in court in keeping with the complex body of legal, policy, and Attorney General Guidelines under which the Bureau operates.

Thus, the FBI faces a task of great difficulty and complexity in building an information technology system that simultaneously meets all three imperatives.

Trilogy after 9/11

Following the attack, the Bureau fundamentally reexamined the project. The earlier, measured approach of June 2001 called for improving legacy systems. In the wake of the attack, the FBI correctly determined that the legacy applications should be replaced to make the Bureau more effective in responding to terrorists' threats as well as to improve the efficiency of the continuing criminal investigative mission.

In the months following 9/11, the Bureau conducted an independent review of available Commercial Off-The-Shelf (COTS) systems and Government developed systems, and determined they could not satisfy the requirements. Therefore, SAIC was tasked to in February 2002 to develop the replacement for the legacy systems using the original contract. The SAIC UAC contract was restructured to incorporate an aggressive development plan first conceived in February 2002. This became the electronic Virtual Case File (VCF) contract. Thus, the FBI shelved 6 months of work that no longer fit the post-911 world, and directed SAIC take on a much more ambitious, high risk project.

The Trilogy VCF was a large and complex enterprise-level undertaking. There are no other criminal investigative management systems of this scale in the world. In terms of size, the VCF DELIVERY 1 system was to manage millions of case files on Day One with an annual growth of hundreds of thousands of cases per year. At start-up, the VCF DELIVERY 1 system was to store and index more than hundreds of millions of documents in a wide variety of formats. The VCF DELIVERY 1 system would support 30,000 users geographically dispersed across the United States and other countries. FBI agents, analysts, and support personnel would rely on the VCF DELIVERY 1 to conduct nearly all the business functions that support the criminal investigative process. The VCF DELIVERY 1 was also to provide hundreds of interfaces to legacy systems. The VCF DELIVERY 1 system would manage this workload while providing a 3-second response to users as well as high system availability. This would not be an ordinary case file management system.

The VCF was intended, in sum, to provide the next generation system supporting the FBI's case file management concept. It would be, as the Justice Department Inspector General has reported, "the first real change in the FBI's workflow and processes since the 1950's". The VCF would move the FBI from its slow, paper-based processes into the twenty-first century with electronic work flow. VCF, it was envisioned, would support real-time coordination among agents, allow secure access to, and reporting of case information for all those authorized to receive it, regardless of organization or location. VCF would support a dispersed community of users in creating, accessing, and managing centrally stored electronic case file information. It would provide the foundation upon which the FBI could migrate its disconnected business processes into an integrated and seamless work environment.

Following the 9/11 attacks, time was of the essence. SAIC was asked to devise an approach to deliver VCF in record time—on an even more aggressive schedule. The new challenge was to define, develop, and deploy a bureau-wide enterprise-level case management system in just 22 months. Without defined requirements or an enterprise architecture for the FBI IT systems, this was a high risk approach that reflected the post 9/11 atmosphere. Here is where SAIC made honest mistakes. We should have made known that this approach was too ambitious.

VCF and "flash cutover"

One of the key issues in the new VCF development strategy was the so-called "flash cutover" approach. That meant, simply, that the new VCF, in spite of its then undefined requirements, would not be implemented via a low risk, evolutionary strategy, but rather would be built as a grand design in record time and be implemented all at once in a "flash cutover" from the legacy systems to the new VCF. SAIC informed the Bureau this was a high-risk strategy. It was here that SAIC should have made its concerns known to the Director. The FBI insisted on this aggressive approach because of its critical need to improve information sharing and case management. SAIC agreed to undertake the challenge. In hindsight, this approach was a fundamental error and, in May 2004, the National Research Council Computer and Telecommunications Science Board was highly critical of the flash cutover approach and instead argued in favor of an incremental deployment model with prototyping and adequate time for test. From 2002 through mid-2004, the Bureau was committed to the flash cutover approach; however, after the Academy report, the Bureau agreed to a low-risk, incremental strategy.

During 2003 and 2004, the Bureau's understanding of how it should respond, of what mechanisms and process it might need, and how it should adjust the IT infrastructure to meet the challenges of fighting terrorism continued to evolve. Not surprisingly, the impact on the VCF program was continuing and significant. In the testimony of the Department of Justice Inspector General before this Subcommittee in March, 2004, the IG identified "poorly defined requirements that evolved as the project developed" as one of the reasons for the delays and cost increases in the Trilogy project. In fact, as recently as 4 months ago, the FBI had a team working to define, confirm, and refine their case management requirements.

When the flash cutover approach was adopted, SAIC formulated an approach to meet the aggressive schedule. SAIC used eight development teams working in parallel and a program staff that reached 250 full-time equivalents. The risks associated with the multi-team, parallel approach became apparent in the fall of 2003. With multiple teams working on vertical slices of the system at breakneck speed, SAIC did not adequately enforce coding standards across the teams and this resulted in less than uniform code. In addition, this approach resulted in some level of duplication of effort in the code with different approaches used to solve similar problems. This, however, did not compromise the system.

Another matter affecting the VCF software development was significant management turbulence. Since November 2001, there have been 19 Government manage-

ment personnel changes that had a direct and significant impact on the management of this project (11 FBI Changes and 8 FEDSIM Changes). This lack of continuity among key Government managers contributed to the problems of ensuring the effective and timely implementation of this system. Each change brought new directions, a different perspective on priorities, and new interpretations of the requirements.

In its report on Trilogy last year, the National Research Council spoke directly to the difficulty of developing software in the absence of specific, settled requirements. As the Council noted, "[I]t is essentially impossible for even the most operationally experienced IT applications developers to be able to anticipate in detail and in advance all of the requirements and specifications."

Probably the most damaging aspect of this development environment was the ever-shifting nature of the requirements. SAIC development teams would meet with the FBI agents assigned to the project to elicit system requirements, then SAIC would translate that into software designs. Often, however, the agents would look at the development product and reject it. They would then demand more changes to the design in a trial-and-error, "we-will-know-it-when-we-see-it" approach to development. The turbulence was not limited to the immediate changes demanded. They would ripple though the related parts of the software design. This cycle was repeated over and over again and prevented SAIC from defining system acceptance criteria and suitable test standards until requirements were finally agreed under VCF IOC this past summer. SAIC expressed concern over the affect of these changes on cost and schedule; however, we clearly failed to get the cumulative effect of these changes across to the FBI customer. We accept responsibility for this failure to elevate our concerns.

The most significant of these changes, occurring during the period when the flash cutover strategy was in place, was to the Records Management System. SAIC had actually selected a commercial off the shelf (COTS) solution and the FBI had agreed to it. Then, late in 2003, FBI representatives decided they wanted a different approach, which would require changes to another COTS software package. The new COTS vendor would not be able to modify the software until a new release of the software was available in spring 2004. At this point, the grand design approach of the flash cutover strategy had begun to fall apart.

In December 2003, we delivered an evaluation copy of the VCF system. The FBI reviewed the product and identified 17 deficiencies, some of which were actually more changes in requirements. These deficiencies and changes were addressed by SAIC, and an updated version of the system was provided in March 2004. The FBI then asked SAIC to assess the cost and schedule impact of incorporating accumulated changes and finishing Delivery 1. SAIC complied with this request in April 2004, but the FBI chose not to undertake this course of action. The goal established early in 2002—define, develop, and deploy a bureau-wide, enterprise-level case management system in 22 months—was now clearly in jeopardy and behind the aggressive schedule.

From VCF to VCF IOC

In May, 2004, a series of meetings between SAIC, the FBI, and FEDSIM took place to define a new strategy. What emerged from these meetings was a significantly different plan.

In these meetings, the Bureau agreed to modify its flash cutover approach in favor of an incremental approach, allowing deployment of new capabilities. Second, instead of replacing its legacy systems at this juncture, the Bureau agreed to focus on creating new capabilities based on legacy systems. Finally, the new approach was christened VCF Initial Operating Capability (IOC) and it was set for Delivery in December 2004. The fundamental understanding between the SAIC senior leadership and Director of the FBI that enabled SAIC to go forward on the VCF IOC was agreement, for the first time, on a fixed set of requirements and defined acceptance criteria.

WHAT THE FBI RECEIVED IN VCF IOC

In December of last year, SAIC delivered VCF IOC. The project was successful. It delivers significant new capabilities, complied with the December, 2004 delivery date, was within the budget allocated for IOC, met 100 percent of requirements established by the FBI for IOC, passed a rigorous testing phase, was accepted by the FBI, meets or exceeds industry standards for quality, and, most importantly, is working well today for FBI agents in New Orleans and Washington Headquarters.

Functional capabilities

With VCF IOC the FBI has a system that will move agents from a slow, paper-based system to a twenty-first century system for their key investigative efforts. In the past investigative information was often held-up in Field Offices, captured in agent notebooks, stored away in filing cabinets, and generally held in different ways and different means all across the country. VCF IOC makes critical information available instantaneously, in a uniform, easy-to-access manner, to all who need to access it regardless of their physical location. Additionally, these new capabilities build a foundation for migrating now-disconnected business processes into an integrated work environment and provide the infrastructure required to add the additional case management capabilities. Specifically, the functional capabilities of IOC include:

—Investigative document import for the FD–302 and related documents (the current mainstay of FBI investigative effort) and National Security Letters.
—Electronic workflow, validation, and approval meeting legal, policy, and Attorney General Guideline standards to ensure admissibility in court.
—Upload of approved investigative documents into the appropriate case files as serials in the legacy Automated Case Support (ACS) system.

Infrastructure capabilities

If widely deployed, the infrastructure capabilities within IOC would take the Bureau from its current paper-based circumstances into a modern web-based environment. Specifically, IOC delivers:

—A modern 3-tier web based computing infrastructure (as a migration target from the legacy mainframe).
—An effective web-based user interface, already well received by agents who have seen and used it.
—Organizational Hierarchy maintenance infrastructure, which matches IT infrastructure to the Bureau's organization.
—Automated interface to the legacy ACS.
—A significant part of the underlying infrastructure for security, access control, auditing and logging.
—System management and integration with the FBI's Enterprise Operations Center (EOC), a 24-7 monitoring and support center.

The functional and infrastructure capabilities in IOC enable the rapid expansion of VCF capabilities, both to add new features and to integrate software developed for Delivery 1 but not included in IOC. As evidence of this, in November 2004, the FBI tasked SAIC to extend the capabilities of the IOC system to provide a significantly broader capability to the Agent users. These extensions were successfully implemented in less than three months and provided to the FBI pilot users, where they have been quite well received.

We believe the FBI would be well served by expanding these capabilities beyond the pilot sites, even as an interim solution to its urgent needs.

Beyond the capabilities and infrastructure active in IOC, SAIC has done substantial work toward meeting the full set of requirements articulated to date for the Bureau and enterprise-wide version of VCF. The product of that broader work can be categorized in three groups. In the first category are capabilities where implementation was complete (or nearly complete), where integration and test were underway, and where routine software problems were being identified and fixed. These specifics of work done in these categories include:

—Case Management
—Leads
—Intake and Report of Investigative Activity (RIA)—which is a different way of approaching the import documents in IOC
—Document Management
—Notifications and Ticklers
—Source Management
—Text Search
—Most of the Reporting Generation Capabilities
—Case Classification Hierarchy Maintenance Infrastructure
—The remainder of the underlying infrastructure for security, access control, auditing and logging including complex business rules address the potentially conflicting pressures to share information post-9/11 and to implement need to know restrictions post-Hansen.

Beyond completing the integration and test effort, additional work would be required to deploy these capabilities focused on (a) resolving outstanding requirements or implementation issues, and (b) adapting the capability away from the flash cut-over approach to the incremental deployment strategy.

The second category represents capabilities where implementation was in progress but engineering or requirements issues required resolution before implementation could be completed, including:

—Evidence Management

—Analysis and Techniques and the remainder of the report generation capabilities.

—Name search

—Resource tracking and management

—Crisis Case management

The third category includes capabilities that were late requirements additions or implementation approach changes and preliminary engineering efforts were in place. This would include records management.

In addition to these capabilities, SAIC performed substantial analysis and engineering efforts to document the complex and largely undocumented legacy environment that has evolved over the years. That effort was critically important to the FBI's information technology initiative. In a December, 2002 report, the DOJ IG noted that the lack of documentation for the legacy systems would limit "how rapidly UAC can be developed and deployed" since "the FBI must know what it has before it can define the right solution to fix the problem". The SAIC team made significant progress in this area producing

—Over 300 Interface Control Documents (ICDs) covering the interfaces between internal FBI systems and also with external systems.

—Extensive analysis and mapping of largely undocumented legacy data to a relational model in preparation for migration into VCF.

CONCLUSION

In conclusion, SAIC has spent the last 36 years working hard and ethically to support important work for the U.S. government and our nation. We have been successful because we have delivered good work for our customers. We followed a difficult path to get there. The Bureau faces difficult choices in difficult and challenging times. Unfortunately, the flawed report from Aerospace Corporation does not provide a sound basis for making decisions about VCF IOC.

The information technology assignment that the FBI envisioned and that SAIC accepted in June of 2001 changed dramatically after the terrible events of 9/11. As the FBI struggled to respond to new missions and conflicting demands, new technology requirements also evolved, and we attempted to keep up. Finally, it became clear to all that the grand design envisioned in the full version of Virtual Case File was collapsing. The FBI agreed, instead, to an incremental approach that would—and did—produce immediate and tangible results. With the delivery of VCF IOC, SAIC has given FBI agents new capability today—not at some uncertain point years from now, but today as they work to combat both crime and terror across this nation.

SAIC pledges to the Committee and to the FBI that we stand ready to work at cost with all parties to recognize the full potential of all of the extensive documentation, analysis and code that has already been provided to further enhance the capabilities of the FBI to perform its vital tasks.

If the FBI's goal is to provide its agents enhanced capabilities as soon as possible and at relatively low additional cost, then we strongly recommend that the FBI continue to deploy VCF capabilities to the agents using the highly successful incremental approach utilized for the VCF IOC delivery and to evolve it along with their emerging enterprise architecture. Using IOC should bring dramatic productivity improvements now while the bureau develops a new system.

If, however, the primary goal has shifted to meeting the new requirements of the new Federal Investigative Case Management System (FICMS), or to adopt the latest technology and COTS components that did not exist when VCF began, then the FBI's agents will have to wait until these new programs deliver as yet undefined capabilities in three or more years. The Trilogy IOC provides much needed capabilities today that are scalable across the entire FBI and provides the foundation to quickly add other required capabilities incrementally over the next year.

PREPARED STATEMENT OF GARY P. PULLIAM, VICE PRESIDENT, CIVIL AND COMMERCIAL OPERATIONS, THE AEROSPACE CORPORATION

Mr. Chairman, distinguished committee members, and staff: I am pleased to represent The Aerospace Corporation and appear before you today as you deliberate Trilogy and the Virtual Case File System.

As a private, nonprofit corporation, The Aerospace Corporation has provided engineering and scientific services to government organizations for over 40 years. We provide a stable, objective, expert source of analysis. We are focused on the government's best interests, with no profit motive or predilection for any particular design or technical solution.

As its primary activity, Aerospace operates a Federally Funded Research and Development Center (FFRDC) sponsored by the Under Secretary of the Air Force, and managed by the Space and Missile Systems Center (SMC) in El Segundo, California. The Aerospace Corporation also undertakes projects for civil agencies that are in the national interest and are consistent with our corporate role. Over 350 staff members focus exclusively on computer systems, software, and information technology.

Our unique "trusted agent" role provided to the Air Force has become known throughout the Intelligence Community. In executing our FFRDC mission, and more specifically, our support to the National Reconnaissance Office, our technical core competencies have become known to the FBI.

1. INTRODUCTION

In 2001, the Federal Bureau of Investigation (FBI) began a major information technology upgrade commonly known as The Trilogy Program. The User Applications Component (UAC) is one of three basic elements of Trilogy. Organizations such as the Government Accountability Office, the Department of Justice Inspector General, and the National Research Council have voiced serious concern about the progress in completing Trilogy, and specifically the UAC. In response to these concerns, the FBI developed and implemented a "corrective action plan" in June 2004. As part of the corrective action plan, the FBI requested that The Aerospace Corporation (hereafter, Aerospace), conduct an independent verification and validation of the UAC; specifically, the Virtual Case File (VCF) Delivery 1.

This testimony summarizes findings and recommendations from the independent verification and validation (IV&V) review of the VCF Delivery 1, conducted by The Aerospace Corporation (Aerospace). This testimony is extracted from Aerospace Report No. ATR–2005(5154)–4, "Independent Verification and Validation of the Trilogy Virtual Case File, Delivery 1: Final Report", delivered to the FBI on January 21, 2005. The FBI, and the Vice President, Civil and Commercial Operations of The Aerospace Corporation have approved release of this information.

This overall scope of the IV&V assessments of the VCF Delivery 1 included the system design, software design, overall security, and the maturity of the development contractor's software development processes. Each assessment comprised reviews and analyses of pertinent documentation, source code, and process-related materials. In addition, the assessment of the maturity of the development contractor's software development processes included a site visit (November 9, 2004) with interviews of key contractor personnel involved in the VCF Delivery 1. The assessments summarized in this testimony were conducted in the period August-December 2004.

It is important to clarify that this effort was not an IV&V in the traditional sense of verifying that all requirements have been satisfied, though requirement satisfaction was part of the assessment. Neither was it an independent program assessment that focused on the entire range of management, programmatic, contractual, and technical issues. Rather, Aerospace conducted a detailed engineering assessment of VCF Delivery 1 requirements and design documentation, source code, and artifacts to provide a recommendation to the FBI on discarding or remediating VCF Delivery 1 products.

Specifically, Aerospace was asked to address the following business questions:

Question 1. Did the incumbent contractor meet the stated requirements?

a. User Needs
b. System Requirements
c. Software Requirements

Question 2. Did the incumbent contractor develop a complete and correct Concept of Operations, System Architecture, and System Requirements?

Question 3. What should the FBI do with VCF Delivery 1?

a. Keep all of it?
b. Keep parts of it?
c. Discard it?

The remainder of the testimony is organized as follows:

Section 2 describes the methodology used in assessing the system design associated with VCF Delivery 1, as well as the software design, security, and the maturity of the development contractor's software development processes.

Section 3 summarizes the findings made by the assessment teams in terms of topics whose state of being influences the answers to the three business questions.

These topical groupings represent (1) architecture, (2) requirements, (3) software quality, (4) performance, (5) security, and (6) contractor processes. More detailed finding statements are found in the Appendices.

Section 4 presents conclusions formed by examining the findings across all six items of interest, as well as inferred findings based on possible observed trends. This section addresses Business Questions 1 and 2.

Section 5 presents a framework for addressing Business Question 3 and a recommendation based on the framework. In addition, general recommendations are given based on Aerospace observations.

2. APPROACH

The IV&V review consisted of assessments of the UAC documentation and artifacts relating to system design, software design, security, and the maturity of the development contractor's software development processes. In addition, the IV&V assessment of the maturity of contractor processes included a fact-finding trip to the contractor's facility to conduct interviews and view additional materials. In general, the methods used were tailored versions of those employed by Aerospace in performing IV&V reviews of national security space systems. The specific approaches utilized by a given assessment team are summarized in the following sections.

Because IV&V is the process of verifying that requirements are satisfied and validating that user needs are met, and because Aerospace was limited primarily to documentation and artifacts, most of assessment was spent examining the quality of and traceability through the documentation and artifacts. This is in keeping with an essential tenet of systems engineering that necessary conditions for a system to be successfully implemented are that (1) documentation and artifacts be complete, clear, concise, precise, and mutually consistent, and (2) requirements be properly decomposed with bi-directional tracing between successive levels of the system (e.g., user needs trace to system requirements, system requirements trace to subsystem requirements, and so forth through design, implementation, and test). Not only do these conditions increase the probability of successfully implementing a system, they are required for effective maintenance.

When possible, the assessment team used industry and government standards as benchmarks against which the program documentation and artifacts were measured. Although standards were not required on the VCF development contract, standards were used in the assessment because they encapsulate known best practices that should be used whether or not they are required of a contractor. The use of standards also eliminates a level of subjectivity from the assessment.

Given the scope and time constraints of the IV&V review, Aerospace focused on a sample of program documentation and other artifacts. Two notable exceptions were that (1) the group assessing the maturity of contractor software development processes conducted a 1-day site visit with the contractor to obtain answers to process questions and to view sample reports and artifacts, and (2) a limited number of Aerospace personnel attended a 1-day design review. In taking this overall approach, it is important to note:

—With the exception of the 1-day site visit and the 1-day design review, Aerospace did not have direct contact with the incumbent contractor to address comments on the documentation and potentially alleviate some concerns.

—With the exception of database performance testing, access was not provided to the tests that occurred or the results of those tests (hence, the review does not directly address how well VCF Delivery 1 satisfies the user requirements but does so by inference).

2.1 System Design Assessment

The system design assessment provided the system-level portion of the IV&V review. The system design assessment was divided into two smaller assessment activities: an evaluation of the system-level documentation (i.e., cross-checking the system-level documentation) and a system-level IV&V appraisal of VCF Delivery 1. The latter consisted of an examination of requirements traceability, requirements satisfaction, performance, and security.

2.1.1 System Level Documentation Assessment

To objectively assess the system-level documentation, Aerospace identified standards against which the documents could be compared. This section describes the ways these standards were used in the assessment.

The CONOPS was reviewed and its content compared against the reference standard embodied in the Department of Defense (DOD) Data Item Description (DID) *Operational Concept Description (OCD)* [1]. (The emerging guide for preparing CONOPS documents [2] that is being created by the American Institute of Aero-

nautics and Astronautics (AIAA), in conjunction with the International Council on Systems Engineering (INCOSE), was also consulted for content and language.) In the review, particular attention was given to the CONOPS with respect to:

—The description of the current system (e.g., operational environment; major system components; interfaces to external systems or procedures; capabilities and functions of the current system; diagrams/charts depicting data flow and processes; quality attributes such as reliability, availability, maintainability, flexibility, extensibility; personnel; support concept for the current system).

—The justification for and the nature of changes (e.g., description of the needed changes; priorities among the changes; changes considered but not included; assumptions and constraints).

—The description of the new system.

—Operational scenarios (e.g., the role of the system and interactions with users; events, actions, interactions, stimuli).

—The new system's operational and organizational impacts.

—The analysis of the proposed system (e.g., summary of advantages; summary of disadvantages/limitations; alternatives and trade-offs considered).

The SADD was reviewed and its content compared to the reference standard found in the DOD DID *System/Subsystem Design Description (SSDD)* [3]. (The *Institute of Electrical and Electronics Engineers (IEEE) Recommended Practice for Architectural Description of Software-Intensive Systems*, IEEE Std 1471–2000 [4], was consulted for content and language.) The SADD was examined with respect to its:

—Presentation of system-wide design decisions. Specifically, decisions regarding system behavior and the selection and design of components; inputs, outputs, and interfaces; actions the system would perform in response to inputs or conditions; description of physical systems; selected algorithms; how databases would appear to the user; approaches to meeting safety, security, and privacy requirements; design and construction choices.

—Descriptions of the system architectural design (e.g., hardware configuration items, computer software configuration items, and manual operations; concept of execution; interface design; requirements traceability).

The SRS was also reviewed and compared against two applicable standards: DOD Military (MIL) Standard (STD) 498, *Software Development and Documentation* [5] and DOD DID *System/Subsystem Specification (SSS)* [6]. (The INCOSE *Systems Engineering Handbook* [7] was consulted for content.) The SRS was assessed against the full breadth of possible requirements, to include:

—Definition of required states and modes

—Internal and external interface requirements

—Internal data requirements

—Safety requirements

—Environment requirements

—Computer-related requirements (e.g., resources, hardware, resource utilization, software, computer communications)

—Quality factors.

In addition to performing reviews of the SADD, CONOPS, and SRS against particular standards, the system-level documentation was assessed for their mutual consistency, completeness, and reasonableness.

2.1.2 VCF Delivery 1 Assessment

2.1.2.1 Requirement Traceability

Aerospace examined the completeness and consistency of user need statements and their maturation into system requirements.

Aerospace extracted all system and software requirements from traceability tables found in the SRS and the SRD, and examined parent-child relationships between these documents. Comparisons were made of each system requirement statement within the body of the SRS to that found in the SRS traceability matrix. A similar comparison was made with software requirements in the SRD.

Validation and verification was performed on subsets of the system-level requirements involving access control and workflow (these requirement areas were chosen, in consultation with the FBI, based on their importance to the UAC). Specifically, Aerospace identified 22 system-level access control requirements and assessed all of them. Of the more than 120 system-level workflow requirements identified, 52 were assessed. The 74 system-level access control and workflow requirement statements were assessed against the following quality attributes provided in *The Engineering Design of Systems* [8]:

—1. *Clear and concise*.—The requirement has only one interpretation and does not contain more than it should. When clarity was in question, the UAC Re-

quirements Terms and Definitions Document (RTDD) was used as the primary source for clarification.

2. *In-scope*.—The requirement does not impose anything unnecessary on the system.

3. *Design- and implementation-free*.—The requirement does not impose a design or implementation solution.

4. *Verifiable*.—The requirement uses concrete terms and measurable quantities.

5. *Free of TBD/TBR*.—The requirement does not contain placeholder statements or values.

6. *Free of conflict or duplication*.—The requirement neither overlaps nor opposes another requirement.

7. *Appropriate decomposition*.—The traced-to software requirements make sense and are complete.

8. *Complete requirement set*.—There is no appearance of missing requirements related to the requirement being examined.

2.1.2.2 Requirements Satisfaction

Actual requirement satisfaction, as determined through a review of requirement testing results, was not considered because test results were not made available. For this reason, Aerospace relied on secondary indicators of requirement satisfaction. For example, the assessment of traceability of the CONOPS, SADD, and SRS was performed within the system-level requirement traceability activity (Section 2.1.2.1), while traceability of software requirements was examined in the software source code and traceability analyses (Sections 2.2.3 and 2.2.5). Other facets of requirement satisfaction were provided by other analyses.

2.1.2.3 Performance

Contractor test methodology and database performance test results, as found in the Interim Scaling and Performance Test Report, were examined to assess the performance of VCF Delivery 1. The goal of the database performance evaluation was to identify areas of high performance risk in the database schema and database Structured Query Language (SQL) query code. Network, application server, and web server performance were not examined.

In addition to examining the contractor test data, independent checks on database performance were conducted through the following means:

—Creation of an Entity Relationship diagram based on the contractor database Data Definition Language (DDL) code, from which further analysis of the database could be conducted.

—Examination of SQL code with respect to (1) system queries, especially with respect to the use of table joins in clauses, nested queries, outer joins, and cursors; (2) code complexity; (3) performance risk factors; and (4) identifying the SQL code critical path [1].

—Review of the database structure for signs of performance enhancement attributes (e.g., table partitioning, table splitting, denormalization, materialized views, and rollup tables).

—Review of the database indexing to determine if table indexes were selected for maximum SQL code performance.

—Analysis of the Virtual Private Database (VPD) implementation performance risks (i.e., looking at the where clause predicates that would be added to each and every SQL query).

—Evaluation of system scalability requirements through an extrapolation of reported test results.

2.2 Software Design Assessment

The software design assessment comprised six distinct analyses: software architecture, software requirements, source code traceability, source code documentation, requirements traceability, and security.

2.2.1 Software Architecture Analysis

The analysis began with a review of the CONOPS, SADD, SRD, Software Design Document (SDD), and accompanying component SDDs. In addition, IEEE Std 1471–2000 [4] was reviewed because it was referenced in the SADD.

The software architecture was examined using an abbreviated form of the Architecture and Tradeoff Analysis Method (ATAM) developed by the Software Engineering Institute [9]. Critical system and software requirements (known as quality attribute requirements in the ATAM) were identified in Exhibit 3–2 of the SADD, re-

[1] Critical path SQL code is defined as those SQL queries that are executed a majority of the time.

viewed, and laid out to form a quality attribute tree, with specification down to the scenario level. (These system quality factors address scalability, extensibility, reliability, performance, security, and evolvability.) Software architectural approaches based on the high priority quality factors were then iteratively elicited and analyzed, with risks, sensitivity points, and tradeoff points identified. Part of the iterative process included brainstorming and prioritizing the scenarios generated in the utility tree based on stakeholder needs (in this case, because access to the actual stakeholders was not possible, the prioritization was based on information in the document artifacts); in the second pass of the process, the scenarios were treated as test cases for the architecture analysis.

2.2.2 Software Requirements Analysis

Software requirements analysis was conducted on data access control and basic workflow requirements after a review of the SRD, SDD (and corresponding volumes), thread design documents, and consultation with the FBI. The quality of these software requirements was evaluated against the following attributes found in IEEE STD 830–1998 [10][2]:

—1. *Unambiguous and clear*.—The requirement has only one interpretation. The UAC Requirements Terms and Definitions Document (RTDD) was the primary source for clarification, followed by Webster's Dictionary [11].

—2. *Consistent*.—The requirements do not conflict, and requirements use the same terms to mean the same things.

—3. *Non-redundant*.—There are no superfluous requirements. Each requirement adds something new to the SRD.

—4. *Complete*.—Nothing is missing from the requirement. Each requirement defines a user type, employs the verb "shall" once, and specifies an end result. Most requirements should also have a performance or timing criterion.

—5. *Single requirement and concise*.—The requirement does not contain more than it should. The requirement has no superfluous detail and expresses only one need.

—6. *Design- and implementation-independent*.—The requirement does not prescribe any design or implementation solution.

—7. *Testable/verifiable*.—The requirement uses concrete terms and measurable quantities. Words like "good," "well," and "usually" signal that a requirement is not testable.

—8. *Complete requirement set*.—No requirements are missing. The set of requirements defines those actions the software will take given all possible types of input data when in all possible states.

Information and findings were shared with and by the system design assessment team to increase overall understanding of critical requirements.

2.2.3 Source Code Traceability Analysis

This section summarizes the combined processes of the source code traceability analysis and the software requirements traceability analysis (Section 2.2.5).

Requirements in the areas of access control and basic workflow were identified and traced from the software requirements to threads and SDD volumes to the source code, using the SDD and corresponding volumes (e.g., Workflow Volume), thread design documents, Test Plan, and the RequisitePro® database. (The initial process of tracing from software requirements to threads was abandoned after the FBI notified Aerospace that the contractor had developed new documentation.) In conducting these traceability analyses, emphasis was placed on:

—Correctness (e.g., does the documented design and source code address the software requirements allocated to it?)

—Consistency (e.g., is the allocation of software to design and code consistent across the documentation and supporting requirements management tools; are allocations at the same level of detail?)

—Completeness (e.g., are all software requirements allocated to design elements and code; do the design elements clearly and concisely satisfy the allocated requirements given the design level of detail?)

Tracings were examined from software requirements through software design and code, and from software requirements to tests.

---

[2] IEEE STD 830–1998 was used because software requirement specifications and system requirement specifications are different, and each has a different set of recommended practices. There is a lot in common between standards for system requirements and IEEE STD 830–1998, and hence duplication, but the two types of standards address different areas of scope for different audiences, and do so at different levels of detail.

2.2.4 Source Code Documentation Analysis

Java source code complexity was determined for all modules. PL/SQL source code complexity was examined for modules related to security, basic workflow, administration, and case management software components. The complexity of modules written in Java was determined using McCabeQA®. ClearSQL® was used for modules written in PL/SQL. Module size, in terms of source lines of code (SLOC), was determined for the respective Java and PL/SQL modules because size is another indicator of complexity. Those modules with the greatest complexity, size, or relationship to other modules were then subjected to a peer review: 191 Java modules, from the functional areas of data access control, workflow, case management, administration, and components, out of 309 high-risk modules; all 667 PL/SQL modules related to the functional areas of workflow, security, administration, and case management, 98 of which were determined to be high risk; and 42 JSP modules in the functional areas of workflow, security, administration, and case management, based on size and relationship to other JSP modules. The underlying source code of the selected modules was compared to contractor documentation (SDD and corresponding volumes, thread design documents, Software Development Plan (SDP)), especially with respect to design and test. Documentation was examined for correctness, consistency, completeness, and suitability. The Java and PL/SQL peer reviews focused on data and control flow, traceability of modules from design documentation, correctness of comments, and other elements of coding practices as defined by the development contractor's coding standards expressed in the SDP.

2.2.5 Requirements Traceability Analysis

The activities of the source code traceability analysis (Section 2.2.3) and the software requirements traceability analysis were tightly coupled. For that reason, the process description and status of the two analyses are combined and reported in Section 2.2.3 above.

2.3 Security Assessment

The security assessment was based on the DOD Information Technology System Certification and Accreditation Process (DITSCAP) [12, 13] and the National Information Assurance Certification and Accreditation Process (NIACAP) [14]. Project documentation reviewed as part of the assessment include the SRS, SRD, SADD, CONOPS, Security CONOPS, SDD, Security Volume, Admin Volume, Security Architecture, Security Plan and associated support package, Privileged Users Guide, and Certification and Accreditation Methodology.

Security-related requirements were identified from the available documentation: the SRS, SRD, and the Security Volume of the SDD. The design of the system was then examined with respect to the subset of requirements to determine the completeness and accuracy of the system design against this requirement set.

Certification and accreditation material contained in the System Security Plan and System Security Plan Support Package was also reviewed to determine its suitability and completeness with respect to what Aerospace experience has shown is necessary for such an activity.

2.4 Software Development Maturity Assessment

The software development maturity assessment was conducted using the same processes Aerospace employs for national security space systems, but tailored to the meet the time constraints of this project. A questionnaire was developed, based on the U.S. Air Force Software Development Capability Evaluation (SDCE) [15], that addresses risks, key requirements, and five areas of specific interest:

—Systems engineering (e.g., system requirements development, management and control)
—Software engineering (e.g., software requirements management, software design, software coding and unit testing, software integration and test)
—Quality management and product control (e.g., quality management, quality assurance, defect control, peer review, software configuration management)
—Organizational resources and program support (e.g., organizational process management)
—Program-specific technologies (e.g., database management, COTS, trusted systems).

Answers to some questions were found in a review of the available documentation: SRS; Master Plan; Configuration Management (CM), Risk Management (RM), and Quality Assurance (QA) Plans; Software Development Plan (SDP); Master Test Plan and Delivery 1 Test Plan; and System Security Architecture. Questions that could not be answered from the documentation, or for which additional information was

needed, were presented to the FBI and the contractor in preparation for an on-site fact-finding visit.

At the time of the fact-finding visit (November 9, 2004) Aerospace interviewed selected members of the contractor staff according to areas identified in the questionnaire. The current Deputy Program Director, who was the VCF Delivery 1 Program Manager, provided interviewees with the questionnaire and scheduled interviews with most of the VCF Delivery 1 managers. The Program Manager accessed the IBM Rational® ClearCase®, ClearQuest®, and TestManager® files during the interview sessions. Time constraints did not permit an in-depth review of the files, but sample reports were printed, and examples of parts of the Software Development Folders (SDFs) were reviewed.

Prior to the visit, Aerospace requested that the following documents and artifacts be available for review: SDFs, the System Engineering Master Plan, documentation from preliminary and critical design reviews, deficiency report databases or spreadsheets, Rational Rose® artifacts, metrics plans and reports, peer review reports, and quality assurance reports. All requested items were made available and reviewed, with the following exceptions:

—The System Engineering Master Plan was not provided. The review team elected not to review it because it was not part of the development contract baseline.
—Rational Rose artifacts were not reviewed. The review team focused on the SDF because coding was accomplished based on the SDF contents.
—No system-level preliminary or critical design reviews materials were reviewed because these events were not conducted. Materials from In-Progress Reviews (IPRs) and the System Requirements Review were reviewed.

3. TOPICAL FINDINGS

The results of the Aerospace IV&V are grouped into six topic areas:

—Architectures (e.g., enterprise-, system-, and software-level architectures)
—Requirements (e.g., concept analysis, system analysis, requirement analysis, requirement quality, traceability)
—Software quality (e.g., software functionality, structure, testing, documentation, thread methodology, database software)
—Performance (e.g., overall system performance of the database)
—Security (e.g., certification and accreditation, system security administration, security requirements definition, security design documentation)
—Contractor processes (e.g., processes defined by the contractor that were or were not followed, processes that worked or did not work).

Findings in each area are summarized in the following sections. Each summary lists strengths and weaknesses, provides a high-level summary of the most important strengths and weaknesses (individually or in groups) and their implications, and gives an overall appraisal of the topic area. Conclusions based on the findings are summarized in Section 4.

With the exception of the software development maturity assessment, all of the assessments were made strictly on documentation and artifacts delivered to Aerospace. This has two consequences. The first consequence is that this usually leads to noting more weaknesses than strengths. If there is sufficient ambiguity or uncertainty of what is intended in a document, a negative finding is generated, even if a short conversation with the contractor could have removed the problem. Therefore, the perceived state of what is being evaluated can be more negative than the actual state warrants. Aerospace did three things to reduce both the likelihood of this happening and the associated impact. First, a fact-finding visit was made to the development contractor's facility to resolve questions about their software development processes. Second, industry and government standards were used to provide objective measures of quality and practices. Lastly, Aerospace looked at both documentation and product (i.e., source code) for possible strengths or weaknesses in each area.

The second consequence of basing the IV&V review largely on documentation is that the ability to transfer the existing document set from the development contractor to a replacement contractor is tested. In this instance many weaknesses could indicate there are significant problems with the documentation or that the concepts being developed are not clearly stated. In either case, it would be very unlikely that a replacement contractor could pick up where the original left off, thereby closing the door on a possible acquisition or maintenance strategy.

3.1 Architecture

This section summarizes the strengths, weaknesses, and Aerospace assessment of the architecture.

3.1.1 Strengths

The incumbent contractor specified a standard three-tiered Web-based design pattern for the VCF architecture. A well-designed and implemented system of this type should be highly flexible, extensible, and scaleable, and should easily integrate new functionality. The theoretical strength of the approach is that it is highly componentized, generic, and built on open standards.

3.1.2 Weaknesses

Though the fundamental strength of the architecture lies in its classic three-tier model, the fundamental weakness relates to the failure to actually implement the system according to the specified architectural concept. As a result, the system risks the ability to maintain, change components (e.g., COTS, GOTS), reuse, or add new functionality to the software. Maintainability and reuse are negatively impacted by the tightly coupled, threaded design. Performance and scalability are likely to be limited by the decision to implement VCF in a centralized versus a distributed fashion. Furthermore, it is possible that certain types of distributed architectures would provide greater reliability through redundancy.

Though maximizing the use of COTS was a stated goal of the VCF program, Aerospace found a limited use of COTS application products, and a design approach whereby functionality available in COTS was rejected, then reimplemented in VCF custom code. In addition, no non-Oracle COTS search and analysis tools were found to be acceptable, as no non-Oracle tools were found to be compatible with the Virtual Private Database and associated access controls.

The use of most COTS software is precluded by the choice for implementation of security and access controls at the data level. The VCF system uses two types of access controls: functional access controls, and data access controls. Functional access controls are implemented primarily in application code written in PL/SQL within the data tier. Data access controls are implemented using the VPD. Because all of the access control mechanisms are enforced by the database, they cannot be utilized by external applications. This is a fundamental limitation in VCF architecture. This means that virtually all functionality available in COTS that requires access control (including document management, workflow, tasking and delegation) must be implemented by developers in the VCF application in custom code. This limitation extends to highly capable COTS search and analysis applications, including link analysis and specialized applications used in other law enforcement and intelligence community applications.

The manner in which the access controls were implemented in the VPD feature of the Oracle database also imposes significant and unacceptable performance delays. While most implementations incorporate some of the controls available in VPD, and apply to a restricted subset of database tables, this implementation uses all of the control mechanisms and applies them to the tables that are used in virtually every join operation required for the response to any normal database query, resulting in significant performance degradation.

Remediation of these weaknesses would require a complete reevaluation of the approach to security access control.

Lastly, the software architecture documentation does not conform to the best practices identified in IEEE Std 1471–2000. For example, stakeholder concerns are not directly mapped to the software architectural responses, there is no viewpoint specification for the software architecture description, a specific methodology is not identified to represent architectural views, and known inconsistencies among architectural description elements are not noted. Failing to adhere to best practices can impact functionality, timeliness, and schedule throughout the development cycle.

3.1.3 Appraisal

Decisions on architecture and the accompanying high-level design are fundamentally important. Yet critical architecture goals have not been met. There was a failure to appropriately assess the use of COTS products. It appears that inadequate attention was given to the performance requirements in relation to the choice of the Virtual Private Database and the associated Access Control List (ACL) table to implement the discretionary access control requirements. Analysis targeted at determining the objects to be protected with discretionary access controls, and methods of protecting these objects, may have resulted in alternate design choices that had more attractive performance characteristics. Likewise, by allowing the original three-tier architecture to collapse to two tiers (thus failing to adhere strictly to the Web-based design pattern), the architectural tenet on separation-of-concerns was violated. Consequently, future technology insertion is at risk, and maintenance and reuse of the VCF software will be more difficult.

3.2 Requirements

This section summarizes the strengths, weaknesses, and Aerospace assessment of system and software requirements (development, analysis, and documentation).

3.2.1 Strengths

All of the system level requirements examined were found to be within scope. There is no evidence of unnecessary features that could constrain design and increase cost.

The System Requirements Specification (SRS) did not contain TBD (to be determined) or TBR (to be reviewed) markings. This is generally a positive indicator for systems that have progressed from the conceptual phase to the development phase, since a lack of TBDs and TBRs usually means that the requirements baseline is stable. However, the lack of TBDs and TBRs provides no assurance that requirements are not missing. Friedman and Sage [16] have pointed out that the lack of TBDs can indicate that requirements have been suppressed or ignored, thus creating what they call "silent specs."

Design and implementation details were not found in either the system-level or software requirements; therefore, the developer adhered to expected system and software development practices.

None of the examined data access control and the basic workflow software requirements duplicated another. Avoiding duplicate requirements eliminates needless requirements analysis and redundancies in development and testing.

3.2.2 Weaknesses

The CONOPS is incomplete in that it lacks summaries of advantages, disadvantages, limitations, and alternatives and tradeoffs considered. It fails to show through analysis that the Information Presentation and Transportation Network Components provide the necessary infrastructure to meet UAC requirements.

The CONOPS does not agree with the SRS, resulting in concepts that are not articulated as requirements in the SRS and requirements that do not correspond to operational concepts. The expected relationship between the CONOPS and the SRS is that the CONOPS should contain statements of operational activities; the SRS should specify system functions through functional requirements. A relationship should exist between the operational activities and the system functions. Contrast this relationship with that between the UAC CONOPS and the UAC SRS: the relationship between operational activities and system functions is missing; there is little correspondence between the statements made in the UAC CONOPS and the UAC SRS functional requirements.

Neither the SRS nor the SRD address all of the requirements expected in a specification. Failure to address the range of applicable requirements can result in a system that is implemented in such a way as to be unacceptable to the user or other stakeholders. Incorporating the additional sections at this point in the life cycle would require a major effort that would subsequently result in rewriting the design documents and making changes to the source code as needed to accommodate these design changes and would result in additional integration and test effort.

The System Architecture Design Document (SADD) is incomplete relative to expectations. Although the SADD lists architecture constraints and goals, it does not describe how the architecture meets them. The SADD includes neither decisions nor rationale for the external interfaces, scalability, extensibility, maintainability, and other items important to the architecture. The incomplete description of the system design could lead to unspecified and untraceable software requirements, which, in turn, leads to a system that does not meet users' needs.

Inconsistencies exist between the Interface Definition Document (IDD), the Interface Control Documents (ICDs), and the SRS. For example, not all ICDs are referenced in the IDD, and some external systems noted in the SRS do not have a corresponding ICD. Although the SRS identifies external systems that currently interface with ACS and the types of interface to be supported by VCF to ensure legacy support, there are no requirements in the SRS that indicate the VCF must ensure such support. The IDD itself contains only seven requirements ("shall" statements), six of which relate to the frequency of interface execution. Inadequate interface definition puts at risk the ability of VCF Delivery 1 to operate with legacy systems.

In addition to reviewing the requirements-related documentation for inclusion of information typically expected in the documents, a quality review of the system-level and software requirements was conducted. Quality deficiencies include problems such as compound requirements, conflicting requirements, ambiguous and undefined terms, use of "and/or" in system requirements, use of "et cetera" in system requirements, use of unverifiable words in system requirements, lack of specified user category in software requirements, lack of response time constraints in software re-

quirements, and redundant system requirements. These quality deficiencies may result in a system implementation that does not meet the expectations of users and other stakeholders. Specific problems and examples are provided in the finding summaries.

The SRS did not completely cover requirements. Gaps in expected system level functionality were found. Additionally, the Requirements Terms and Definitions Document (RTDD) contained implied requirements. Placing implied requirements within the RTDD does not ensure that the expected functionality will be implemented.

Traceability was assessed on various levels and from various perspectives. The expected relationship between need statements, system requirements, and requirements for lower-level elements (e.g., hardware and software) is that there is a strict downward flow of requirements. Every need statement maps to a system requirement and every system requirement maps to a need statement. Thus, there are neither "childless" need statements nor "orphan" system requirements. The process continues in a like manner for the system requirements and lower-level element requirements. Contrast this with what is observed in the UAC need statements and requirement documents: need statements do not flow exclusively to system requirements, and in many cases they bypass the system requirements completely. The lack of traceability from need statements to system requirements could result in a system design that does not meet user needs and may implement features that are not required.

Traceability was also assessed in the SRS review by conducting a decomposition analysis on a set of requirements from the SRS to the software level. The analysis identified problems such as incomplete decompositions and decompositions that were more restrictive than the system level requirement. Additional traceability analyses assessed the mapping of system and software requirements to the traceability matrix; errors were found in the trace. The mapping of business rules to software requirements was also incomplete. Here again, the lack of traceability from system requirements through design means that the design may not meet requirements and may implement features that are not required.

Finally, analyses were conducted of traceability from software requirements to software design and source code, and from software requirements to tests. There were three sets of artifacts that provided traceability between the software requirements and the design: the RequisitePro® database, the thread documents, and the SDD volumes. The RequisitePro® database traced to the name of a thread, which was associated with the corresponding portion of the SDD volume for basic workflow and for data access control. The RequisitePro® database was consistent with the traceability in the SDD volumes (with one exception), but not consistent with the traceability in the thread documents. It is Aerospace's understanding that the thread documents were the original design documents and that the SDD volumes reflected the as-built software. All but one of the software traceability findings deal with the SDD volumes as opposed to the thread documents.

There was poor traceability from the software requirements for basic workflow (BW) and data access control (DAC) through the design to the software components. A spot-check analysis of the workflow code shows that some software requirements do not appear to be covered in the code itself. There are some DAC software requirements that are inconsistently traced between the RequisitePro® database and the Security Volume of the Software Design Document. Lack of adequate requirement traceability into software design and code results in risk that the software will not meet its stated requirements and greater difficulty of modifying software when requirement changes occur.

There were several BW software requirements that were not assigned to tests in the Delivery 1 Test Plan. Without these requirements being validated in assigned tests, there is no certainty that the users' requirements are completely met.

3.2.3 Appraisal

The requirements, analysis, and documentation associated with the UAC and VCF Delivery 1 contain significant information deficiencies that must be corrected to ensure an adequate system definition and development process; a majority of the system and software requirements examined contain quality deficiencies; and the requirements decomposition and traceability chain, from the SRS to SRD to software design components to source code to test documents, is weak because of missing information and inaccuracies. Extrapolating these observations to the entirety of the requirements, analysis, and documentation leads to serious concerns about the maintainability and reusability of VCF Delivery 1. Remediation could be very time-consuming and, because of the traceability concerns, may not ensure that all problems would be addressed.

3.3 Software Quality

This section summarizes the strengths, weaknesses, and Aerospace assessment of the software, to include database software.

3.3.1 Strengths

VCF Java Package Standards, set forth in Appendix A of the Software Development Plan, were followed. In particular, the Struts framework was followed, compelling developers to follow a Model View Controller design. This was significant because developers familiar with Model View Controller design and the Struts framework should be able to understand the flow of information in the source code and maintain the presentation layer of software with little difficulty. Also, the software components described in the Workflow Volume of the SDD were almost all found in the code. This is important for maintenance purposes.

3.3.2 Weaknesses

Commenting standards were not consistently followed in the source code files that were analyzed. For example, very few functions or files included a change history, and there were no references to the design documents associated with each class. This inconsistency indicates that coding standards listed in the Software Development Plan were not always followed. Not following a formal software development process for such a large system implies the lack of a disciplined approach, a lack of coordination among developers, and a lack of standards enforcement. The result of inconsistent comments is that the burden of source code maintenance increases because programmers are forced to search through the documentation every time the code needs changing or when checking for possible side effects associated with making changes to different classes. This weakness can be corrected only by going through all the source code files and writing the needed comments. There are also comments in the code that mention work that remains to be done. This means that either the code is incomplete or that the misleading code documentation was never removed from completed code. This code should be examined in detail and compared to the design to determine its status, and it should be tested to be sure it ran without errors. Then these comments should be removed to eliminate confusion.

Some Java classes have modules with incomplete code and unused code. This code cannot be validated because its purpose is unknown. Such code can affect the safety of the system by performing unexpected and unplanned operations. If the code is not fully validated, then the proper operation of the system cannot be assured.

Some Java code contains inconsistent use of constants by hard coding and some by using constants and database files for others. The preferred method is to use constants and database files so that any future changes can be made to the constant or to the database, thereby ensuring completeness of the change. Hard coding requires that changes be made to all instances and some may be missed.

Discrepancies were found between the thread design documents and the Software Design Document volumes for data access control and basic workflow. In addition, there were cases where more detailed design was found in the thread documents than in the design documents. Inconsistent design documentation is confusing to anyone trying to understand, maintain, or modify the software.

The design documentation reviewed does not bridge the gap between the Software Design Document volumes and the source code. Missing design information included the relationships between the software components; class parameter details; full definition of class interfaces; and details on the purpose and logic of each function. The existence of the code is listed in the high-level design, but not the code behavior and interactions, which should be reflected in the lower level, detailed design. Examples of missing design details include: (1) the PL/SQL code for workflow contained a total of 111 modules, of which 57 were not mentioned in the SDD; (2) a discrepancy between the Java files listed in the SDD volumes and the source code provided to Aerospace. The lack of a detailed design document that included all source code modules makes maintenance and modifications to the source code more difficult and time-consuming, and would subsequently drive up the cost of any future changes to the system.

The PL/SQL code has timing and design issues. With regard to timing, each module writes a character string to the debug log (in one module printing is initiated through the use of a debugging switch; in all other cases the printing is hard coded). This has a negative impact on code performance because it increases execution time; this practice would be tolerable only during prototype development. As to design, the PL/SQL code uses literals rather than symbolic constant variables in the arguments of "IF" and "WHERE" statements. This code would be nearly impossible to maintain by anyone other than the programmer who developed it because there are no references to design documents that define literals, such as the integer-type val-

ues. This is an example of not following coding standards, or of not enforcing them. It would take time to fix this code properly by replacing the literals with symbolic constant variables so that it could be understood by anyone other than the original programmer.

3.3.3 Appraisal

The source code appears to have been produced without adherence to the procedures and standards stipulated in the Software Development Plan. The source code examined is not maintainable with its current documentation. Without reverse-engineering the missing documentation and conducting thorough testing, the code should not be used for any operational system. To reverse-engineer this system to bring it up to the level for proper maintenance and support would cost about one-quarter to one-half of the original cost of development. In most systems, 15 percent of the cost is derived from the documentation across all development stages. Testing, including documentation, typically accounts for 40 percent. Approximately half of the documentation needs to be completed. The remaining testing is expected to be between half and all of the cost of a typical system. This depends on problems found during testing.

3.4 Performance

This section summarizes the strengths, weaknesses, and Aerospace assessment of system and database performance.

3.4.1 Strengths

None identified.

3.4.2 Weaknesses

The VCF system that was tested by the contractor was a development version (VCF Delivery 1), which is missing requirements and is inadequate for operations. The system did not implement a number of features, such as the Virtual Private Database (VPD) or full production scale of hundreds of millions of rows in the database. The measurements (as documented in the Interim Scaling and Performance Test Report) only present some CPU utilizations and end-to-end response times from/to the web server. Disk, bus, and network actual performance were not provided in the performance report provided to us and are presumed not to have been tested.

The reported system performance and its performance analysis approach are at best marginal. Only the least-complex transactions were reported, and a number of those did not meet requirements even for the scaled-down database without VPD. A fully populated production VCF system based on VCF Delivery 1 would not meet requirements. In some cases the response time would be hundreds of percent longer than is required, and in worst cases thousands of percent longer than is required. Such long response times are essentially nonresponsive.

The VCF database has the attributes of a logical database model with large numbers of tables, a lack of denormalization, subtype entities modeled directly to physical tables, and other logical data model features. Logical models are rarely performance-optimal. The typical database objects available for performance optimization (e.g., performance-based index selection, materialized views, table partitioning) are absent from the VCF database. At the current estimated row counts, the database will require heavy optimization in order to scale properly; however, the developers did not do this.

The database load estimates were created using historical ACS usage. While using historical ACS usage was a good starting point, a more thorough analysis of the probable usage of VCF should have been performed before translating these estimates into a testing protocol.

The database SQL code is not performance-optimized. The SQL code throughout the system uses many of the constructs that are specifically noted in the database manufacturer documentation [17, 18] as being performance risks. Compounding the problem is the use of the Oracle VPD feature for database security. The VCF implementation of this feature causes even more poor-performing SQL code to be added to each and every SQL statement in the database.

The executed performance tests were flawed in two ways. First, the contractor did not isolate the database when the CPU utilization was tested. Aerospace was unable to conclude whether the database CPU was underutilized because it was not having a problem with servicing requests or it was waiting on another dependent system. The database CPU could also have been waiting on internal database hardware such as bus data transfers. The second flaw in the performance tests is that the test database was loaded at substantially lower row counts than what is estimated as needed, even for the ACS database migration.

An enterprise such as the VCF requires to be managed by a Network Operations Center (NOC). The NOC would include a Network Management System (NMS), archiving, availability monitoring, and other system and operational functions.

The NMS would include functions such as a help desk, trouble ticket system, a network management console, and network management agents on the managed workstations and servers. The NMS would use protocols such as SNMP (Simple Network Management Protocol), RMON (Remote Monitoring), and others. The lack of a requirement for an NMS would result in a system that cannot be operated in a production environment, especially after it is fully scaled to global production size. Any production system requires routine archiving. Most systems have an incremental or even a full backup daily, and a full backup at least weekly. Without archiving, work could be lost, evidence misplaced or destroyed, and investigations could lose their integrity. The lack of a requirement for archiving would result in a system that cannot be operated in a production environment, especially after it is fully scaled to global production size.

Any production system must meet availability requirements commensurate with its mission. A system that is unavailable could result in an interrupted investigation due to lack of access to investigation data, or the inability to record new information that is crucial to progress in the current investigation and other affected investigations that depend on new evidence collected. On top of that, investigation resources would be lost when the system is down. The lack of a requirement for system availability would result in a system that cannot be operated in a production environment, especially after it is fully scaled to global production size.

3.4.3 Appraisal

The system falls short of meeting requirements as tested. In addition, the scaled-up system, with the VPD running, is highly unlikely to meet requirements, particularly for the type of complex queries needed by VCF. Simple queries would be hundreds of percent slower than the type of queries that were tested by the incumbent contractor. The situation would be far worse for complex queries running on the scaled-up system. The system would fall short of requirements with extremely long response times—thousands of percent longer than is required. Such long response times are essentially nonresponsive.

The database has many characteristics of a database still in development: a physical implementation of the logical database model that will undergo significant modification well before production, and SQL coding statements structured in a way that is logically sound and easily understood, but not optimized for performance. Developers typically develop code in this manner, expecting that time will be allocated to performance optimization once the code is functionally correct. Code modifications are also easier before optimization.

The database hardware selection appears adequate for the raw amounts of data that must be processed, but the database subsystem requires a realistic test with all features active, especially the VPD security and a full ACS migration data load. The production hardware and COTS software (i.e., Oracle database, Sun server, and the Hitachi Storage Area Network (SAN)) are technically capable products. However, the current VCF database schema and SQL code implementation do not contain the performance enhancements that would allow the hardware and COTS database server to perform optimally.

3.5 Security

This section summarizes the strengths, weaknesses, and Aerospace assessment of security.

3.5.1 Strengths

It appears that planning for system security was done at a high level early in the program. Such planning increases the likelihood that required security features (e.g., access control, audit) will be addressed in the requirements and design, which, in turn, provides a cost-effective path to certification and accreditation. Select areas of the system not generally found in initial system security reviews (e.g., infrastructure devices such as routers and switches that nonetheless contain functionality that must be addressed from a security perspective) were addressed in some amount of detail.

The system design provides for a limited interface controlled by the VCF application and infrastructure (for non-administrative users to interact with the VCF). This approach prevents exposure to security vulnerabilities that may exist in the interfaces provided by underlying products (not visible at the user interface), such as the command line for an underlying operating system.

At a high level, these strengths point to an approach that, if followed, would produce an accreditable system.

3.5.2 Weaknesses

Several weaknesses were discovered that create a significant risk that the system will not be accreditable.

Broad areas of security requirements were neither well-defined nor correctly decomposed to lower-level requirements. Although the coverage area of the lower-tier requirements was the same as that in the higher-level documents, the lower-tier requirement did not provide the necessary detail to implement and test the system in support of the certification and accreditation effort. Furthermore, the documents identified as the primary means for the certification and accreditation effort (the System Security Plan and the System Security Plan Support Package) did not map to the requirements specified for the system. This failure to identify the requirements to which the system would be accredited greatly increases the risk that the system would not receive accreditation, even if built to the requirements specified. Weaknesses were found in design and implementation. The Privileged User Guide should contain information to manage and configure the system in a secure manner. However, there are many sections marked TBD, as well as sections that do not provide the detailed procedures required to perform critical configuration steps (e.g., specific configuration instructions for the boundary devices so that fundamental assumptions noted in higher-level documents can be achieved). Some of the detail provided in this guide also appears as if it were copied from other sources, and not modified for application to the VCF system. Without specific configuration information, the trustworthiness of the system cannot be assessed and the system will not be accreditable. Furthermore, if the security features that are needed do not exist, or do not support all of the capability being depended upon by the architecture, then significant schedule and dollar costs will be incurred.

The design documentation for the audit subsystem does not describe how the audit requirements are being met, especially in the area of management of the audit trail. While the Privileged User Guide contains COTS audit configuration steps, there is no discussion concerning how the VCF audit is managed, and how the VCF audit can be integrated with the audit trails produced by the COTS products to provide a coherent audit trail.

3.5.3 Appraisal

At a high level, the system security description appears to be a good start in describing the functionality necessary to build an accreditable system. However, in specifying and designing the system to meet that functionality, it appears there are significant shortfalls. Select requirements specifying the functionality are imprecise and incorrectly decomposed. The design of critical identification and authentication and audit subsystems do not implement a significant portion of the requirements for those subsystems. The documents supporting the certification and accreditation of the system and security configuration are not complete.

While all of these issues can be remedied, at this point in the product lifecycle there is a high risk that the system implementation will not meet the security requirements, and that significant additional costs (both to the schedule and in dollars spent) will be incurred in trying to address the issues identified. There is a high likelihood that the system as it currently stands will not be able to be accredited without significant additional effort on the part of the developer.

3.6 Contractor Processes

This section summarizes the strengths, weaknesses, and Aerospace assessment of the contractor processes.

3.6.1 Strengths

Strengths regarding the development contractor's initial processes include:

—Good organizational structure for program management and quality assurance
—Selection of requirements, software, and documentation control tools
—Use of peer review and audits as key elements of the quality assurance process
—Good configuration management and integrated management tools
—Tracking of change requests.

A Chief Engineer was designated to monitor the development and integration of the systems engineering, software engineering, and data engineering activities. The Quality Assurance Manager reported to the Group-level QA at a level above the Program Manager to provide independent quality assessments of compliance with the established procedures.

Processes and procedures for the software development were defined and documented in the Software Development Plan. COTS tools for managing these processes were selected and are the same as those used frequently in other government developments. Configuration Management to control and track the baselines and

changes to the requirements, documentation, and software was defined and controlled via an integrated, automated tool suite.

3.6.2 Weaknesses

The Master Plan did not include planning information (such as key events and tasks) and controls (such as system level reviews) for the development task. The implemented risk management process included only an ad hoc risk identification method—personnel identified perceived risks to the Risk Management Board for analysis. Although the organizational structure provided for integration of the engineering tasks, there was a lack of engineering discipline as evidenced by the lack of adherence to established processes.

The software methodology did not provide for the database design, implementation, and test. There were neither top-level software descriptions nor interfaces depicted in the Software Development Plan. The database was developed after the software design, which led to performance problems. Software integration testing was not planned for in the Software Development Plan, and the test plans called this by different names without describing how it was to be done. The system integration manager and team did the software integration testing, but this was not made clear in the documentation.

Requirements were tracked and reported in the RequisitePro® tool, but software requirements were not traced to the code—only to the threads (which is at a very high level).

The quality assurance (QA) program did not include QA activities for the software code; QA only checked that the peer review process was followed.

Software development folder guidelines were published in the SDP and in the Minimum Thread Team SDF Layout and Contents, but did not provide for a convenient structure to maintain the artifacts. SDF files were dispersed in several different tools and in many folders, making it difficult to find a complete SDF.

3.6.3 Appraisal

The major process strength of VCF Delivery 1 was the documenting and planning for the guidelines, procedures, and process controls in the beginning of the program in the Software Development Plan. The major weakness was a lack of compliance and completeness in the procedures.

The SDFs were used to maintain the updated requirements analysis, design materials, implementation artifacts, testing results, and lessons learned. The SDFs were to be the key documentation since the other documentation was not updated. However, assessing the completeness of the SDFs is extremely difficult and cannot be done without detailed guidance from a developer.

A major defect for the maintainability, reusability, expandability, and reliability of the VCF Delivery 1 software is the lack of a defined and documented software architecture and software methodology. Without the tracking of requirements to the software, the reliability and usability of the system is questionable and the software cannot be verified and validated. Without good software architecture, there is no structure to build for future development or functionality.

4. CONCLUSIONS

The principal conclusion of the IV&V effort is that a lack of effective engineering discipline has led to inadequate specification, design, and development of VCF Delivery 1. Most of the findings presented in Section 3 relate in some way to this conclusion. From the documents that define the UAC 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 engineering practices followed on this program were not in keeping with what Aerospace would expect in a program of this magnitude and importance. Good engineering practice includes, of course, well-written requirements that specify the essential functionality, performance, and constraints of the system. It also includes

—Modeling to analyze behavior and performance, and to ensure the correctness, completeness, consistency, and realism of the requirements

—A correct decomposition and flow down of requirements from user needs to system requirements to design.

These practices were found lacking or ineffective for the VCF program. Without them there can be little assurance as to the correctness and completeness of the requirements and design.

Secondary conclusions address two of the FBI business questions stated in the Introduction. Business Question 2 asks, "Did the incumbent contractor develop a complete and correct Concept of Operations, System Architecture, and System Require-

ments?" and speaks to the framework of the UAC system and VCF Delivery 1. Business Question 1, on the other hand, asks, "Did the incumbent contractor meet the stated requirements?" and must be considered in light of user needs, system requirements, and software requirements. Responses to these questions are not given in terms of a simple "yes" or "no," but are phrased in terms of assurance of an affirmative answer.

The secondary conclusions, together with their basis in the findings, are given below, as well as the summary assessment of the state of the UAC and VCF Delivery 1.

4.1 Regarding the Quality of the CONOPS, Architecture, and Requirements

Findings in the areas of architecture and requirements indicate that the concept of operations, system architecture, and system requirements were not sufficiently mature for the purposes of developing VCF. The SRS does not provide an adequate basis for the developer to design the system. The SRS and the CONOPS taken together do not provide a complete and consistent view of the system. The SADD contains certain sound architectural concepts but fails to adequately consider the use of alternate architectural concepts or the use of COTS that may have better served the needs of the VCF system. Therefore, Aerospace finds no assurance that the architecture, CONOPS, and requirements are correct and complete, and no assurance that they can be made so without substantial rework.

4.2 Regarding the Satisfaction of Requirements

Findings on user, system, and software requirements touch most of the areas of interest (i.e., architecture, requirements, software quality, security, and performance), and tend to be negative. Based on the requirements examined, the findings indicate that a substantial body of requirements are imprecisely written or incorrectly decomposed into lower-level requirements, detailed designs, or test scenarios. There are key requirements whose correctness is questionable, and there are notable instances where the design and implementation do not match the architecture and requirements. The extent of requirement satisfaction could not be fully determined because only high-level test plans, software problem reports (SPRs), and a performance test report were available; other documents that are normally examined in determining requirement satisfaction (e.g., requirement test plans and procedures, and results from testing) were not available. There is no evidence that the system will scale to the storage and throughput capabilities under the demands of a fully loaded scenario; rather, evidence was found to the contrary. Therefore, Aerospace finds no assurance that requirements, at the system or software level, will be fully satisfied, and no assurance that they can be satisfied without substantial rework.

4.3 Overall Assessment

The UAC and VCF Delivery 1 do not adequately meet system and software requirements. Each of the six areas examined has significant weaknesses and few compensating strengths. For example,

—The architecture was developed without an adequate assessment of alternatives and conformance to various architectural standards, in a way that precluded the incorporation of significant commercial-off-the-shelf software, and without modeling and simulation to determine whether the architecture would meet user needs in realistic situations.

—High-level documents were neither complete nor consistent, and did not map to user needs.

—Requirements and design documents are incomplete and imprecise, requirement and design tracings have gaps, and software cannot be maintained without difficulty, and is therefore unfit for reuse.

In short, VCF Delivery 1 is a system whose true capability is unknown and may be unknowable, unless substantial time and resources are applied to remediation.

5. RECOMMENDATIONS

This section presents a framework for addressing one of the FBI business questions set forth in the Introduction and recommendations based on the framework. Additional recommendations beyond the scope of the original business questions are also provided.

5.1 A Framework for Addressing FBI Business Question 3

FBI Business Question 3 asks, "What should the FBI do with VCF Delivery 1?" The possible outcomes include keeping all of it, keeping parts of it, or discarding all of it. Although this independent assessment is primarily technical in nature,

stakeholder interests that affect the disposition of VCF Delivery 1 may be technical, budgetary, schedule-based, or mission-oriented in nature. Only the FBI—in consideration of the various stakeholder interests—can make the ultimate decision on the disposition of VCF Delivery 1.

The decision to be made about VCF Delivery 1 is framed by the conditions that must be met in each possible outcome. As understood by Aerospace, the outcomes and conditions are as follows:

—Under what conditions should the FBI keep VCF Delivery 1?
  —Only if VCF Delivery 1 satisfies all requirements or remediation is readily achieved.
  —Only if the FBI desires a custom UAC solution versus a solution based on COTS software.
  —Only if it satisfies the needs of the FBI with respect to functionality, schedule, affordability and life-cycle issues.
—Under what conditions should the FBI keep parts of VCF Delivery 1?
  —Only if there are separable components of VCF Delivery 1 that contain useful functionality in the future context of the UAC.
  —Only if VCF Delivery 1 meets the conditions for reusable or maintainable software.
  —Only if the FBI still desires a custom VCF solution versus a solution based on COTS software.
—Under what conditions should the FBI discard VCF Delivery 1?
  —Only if VCF Delivery 1 satisfies none of the conditions above.

5.1.1 Regarding the First Possible Outcome

Regarding the first outcome, keeping all of VCF Delivery 1, Aerospace has no assurance that the VCF Delivery 1 requirements have been met or that remediation may be readily achieved. In fact, Aerospace concludes that determining which requirements are actually met and remediating those that are not would be very costly and time-consuming, given that there are serious concerns with every level of the system, from the requirements and architecture, to the design and the software.

5.1.2 Regarding the Second Possible Outcome

The second outcome, keeping parts of VCF Delivery 1, depends on whether components of VCF Delivery 1 will be useful in some future context. In the current context, VCF Delivery 1 is custom software based on a centralized hardware architecture. Thus, if the future context is a COTS-based service-oriented architecture (SOA) solution based on a distributed hardware architecture, it is less likely that useful components of VCF Delivery 1 will be found. On the other hand, if the future context is another centralized hardware architecture with custom software, it is more likely that useful components will be found. This last instance is precisely the context in which the incumbent contractor is developing the IOC software—and is, in fact, reusing components of VCF Delivery 1.

Even if a future context occurs in which components of VCF Delivery 1 are deemed useful, Aerospace has concerns on the reusability and maintainability of the software based on the documentation, design, and coding standards. The software was not written for reuse and has serious maintainability and extensibility problems as well.

Because the Aerospace IV&V review was based largely on documentation and artifacts, and included no substantive direct contact with the development contractor other than that needed to assess the software development processes, the ability to transfer the existing document set from the development contractor to a replacement contractor was tested. The many documentation weaknesses that were found indicate the existence of significant problems. It is very unlikely that a follow-on VCF contractor could pick up where the incumbent left off, thereby weighing against this as a possible acquisition strategy.

5.1.3 Regarding the Third Possible Outcome

The third outcome, discarding all of VCF Delivery 1, is essentially the default condition that will occur if none of the preceding conditions are met. It can be reached if the VCF Delivery 1 software is found unsuitable for reuse and beyond remediation. Alternately, it can be reached by fiat if the FBI should decide—based on the results of the Aerospace COTS/GOTS survey [19]—to proceed with a COTS-based solution.

5.1.4 Recommendation

It is evident from this decision framework that the VCF Delivery 1 decision depends on more than just VCF Delivery 1 itself. It depends on the total future context in which the VCF application will exist.

It is clear that the first outcome (keeping or remediating VCF Delivery 1) is not feasible because of the lack of assurance that VCF Delivery 1 fully satisfies the system and software requirements, and because Aerospace can foresee no condition under which remediation would be feasible. Put another way, any remediation of VCF Delivery 1 would be akin to starting over.

The second outcome (keeping parts of VCF Delivery 1) is more feasible than the first, but is still fraught with difficulty. Because VCF Delivery 1 documentation and source code do not meet the conditions for reusable or maintainable software, Aerospace believes it would be difficult for any contractor (including the incumbent) to extract much of value from the current requirements, design and software given the poor state of the documentation. Furthermore, Aerospace believes it would be extremely difficult for any contractor besides the incumbent to do so.

Additionally, using VCF Delivery 1 or a derivative thereof only makes sense absent a preference for a COTS-based VCF solution. Given that there are multiple COTS applications, or features within applications, that meet the needs stated in the Federal Investigative Case Management Request for Information (RFI) [19], the question of reusing parts of VCF Delivery 1 rests on:

—Having functionality that is superior to the COTS options or that is not available in COTS;

—Having functionality that is modular and has a defined interface application programming interface (API);

—Its ability to provide a clearly defined service or set of services in the context of an SOA. Both the RFI and current federal information technology acquisition guidelines (Clinger-Cohen Act [20], Federal Enterprise Architecture Guidelines [21]) stress the desirability of SOAs.

While the discussion to this point is implicitly about the best long-term VCF solution, it is also worth considering what may be a useful short-term solution. It may, for instance, be the case that the work currently being performed by the incumbent contractor on an IOC build will provide a short-term capability to satisfy mission needs in a timely fashion until a solution can be crafted that is both more capable and more feasible for the long term. Whether or not this is feasible depends on the timeliness and affordability and short-term utility of an IOC-like solution versus the timeliness of a COTS-based solution (which is a strong contender for the preferred long-term solution).

Thus, pending the outcome of the trade studies recommended below, Aerospace believes that discarding VCF Delivery 1 and starting over with a COTS-based solution is the best long-term solution. Although Aerospace recommends that VCF Delivery 1 not be used as a software baseline for any future VCF activities based on the deficiencies identified herein, Aerospace recommends that the VCF Delivery 1 artifacts (both documentation and source code) and this report be made available as Government Furnished Information[3] (GFI) to any future VCF vendors (as part of a "Bidders' Library" for instance). There are insights to be gained from understanding how the VCF problem was initially framed, how the architecture was conceptualized, and how the system was designed and implemented that Aerospace believes will be of use to future developers. Aerospace recommends, however, that these artifacts be made available only if accompanied by this report. Otherwise, the future vendors will be in the position of having to repeat all the investigation and analysis performed by Aerospace in its investigation of those artifacts.

Based on the RFI responses, there are multiple COTS applications, or features within applications, that meet both the SOA requirements and the needs stated in the RFI.

5.2 Additional Recommendations

The fact that Business Question 3 was asked at all implies that the future of VCF is being considered. The larger issue, then, beyond the disposition of VCF Delivery 1 is the way ahead for VCF. It is in consideration of this larger issue that the following recommendations are offered.

The principal conclusion of this assessment relates to a lack of engineering discipline and all its negative effects. Accordingly, this problem must be remedied before going forward. Broadly speaking, this will require that the FBI specify that appropriate systems engineering and software engineering practices be defined and used, and then provide oversight to ensure that they are followed. Allowance must be made for a reasonable schedule. An assessment conclusion states: "The engineering practices followed on this program were not in keeping with what one would expect in a program of this magnitude and importance." The specific recommenda-

[3] Providing the documents and artifacts as Government Furnished Equipment (GFE) is not recommended so as to avoid the government incurring any liability for their use.

tions offered below speak to practices that Aerospace believes are in keeping with a program of this magnitude and importance.

5.2.1 Concerning the VCF Architecture

Aerospace found that VCF Delivery 1 began with certain sound architectural concepts, but failed to consider the use of alternate architectural concepts or the use of COTS components that may have better served the needs of the VCF system. Therefore, Aerospace recommends that trade studies be performed across several key dimensions, to include the following at a minimum:

—The use of COTS components for key integrated case management functionality (not merely for infrastructure items such as databases, operating systems, and communications protocols) versus the use of custom application software.

—The use of an SOA versus the use of a monolithic software application.

—The use of a distributed hardware architecture versus the use of a centralized hardware architecture.

Additionally, Aerospace recommends an analysis of how VCF fits in with, and is constrained by, the broader enterprise architecture.

5.2.2 Concerning the VCF Requirements

Aerospace found the VCF Delivery 1 concept of operations and the system requirements to be insufficiently mature for the purposes of the UAC acquisition. Therefore, Aerospace recommends that a new series of meetings be conducted with the users and other stakeholders to elicit needs, constraints, operational concepts, and requirements. Once a set of abstracted needs, constraints, and broader enterprise concerns is in place, it will be possible to perform the operational and requirements analyses, modeling of operations and functions, and modeling of performance necessary for the creation of a correct and complete CONOPS and System Requirements Specification.

Aerospace found a lack of accurate and complete traceability between the various levels of requirements, components, and tests. Therefore, in order to provide assurance that all VCF requirements have been met and verified, Aerospace recommends that the any future VCF development and acquisition activities enforce strict traceability.

5.2.3 Concerning the Use of Standards

Many of the problems with the body of VCF documentation extend beyond a simple lack of discipline and instead relate to a failure to address certain standard concerns in system architecture, system specification, system design, and requirements quality. The systems engineering field is sufficiently mature that there are standards and other references that provide descriptive outlines for key documents and quality attributes for written requirements.

Many—though not all—of these standards originate in the defense arena. However, they are applicable (with tailoring) to non-defense systems such as VCF precisely because it is similar to many defense systems in its complexity, its scope, and the criticality of its mission. As such, the approaches used in creating other large, complex, mission-critical systems can be applied here. The standards and other references that Aerospace applied to the VCF assessment are given in the bibliography contained in this document. Aerospace believes they are as applicable to the future of VCF as they were to an assessment of its past.

5.2.4 Concerning Processes

The success of acquisition programs, particularly large ones, depends not only on what is done but also on how it is done. Products result from processes—and it is precisely for this reason that processes are important. While a good process is not sufficient to produce an excellent product, it is necessary.

A project of the scope, complexity, and importance of VCF demands the level of process maturity embodied in CMMI Levels 3 and 4. CMMI Level 1 and Level 2 are too "ad hoc" for a program of this nature; on the other hand, CMMI Level 5 is probably not warranted.

Aerospace recommends that a Software Development Capability Evaluation be conducted prior to contract award to reduce acquisition risk by objectively assessing each offeror's ability to successfully develop the software needed by the VCF program. Aerospace recommends that an independent government cost analysis be conducted during source selection to objectively assess the cost realism of each offeror's proposal.

REFERENCE

[1] U.S. Department of Defense. *Operations Concept Description (OCD)*, Data Item Description DI–IPSC–81430, December 5, 1994.
[2] American Institute of Aeronautics and Astronautics, *Guide for the Preparation of Operational Concept Documents*, Working Draft 1.0, ANSI/AIAA G–043–200x. Washington, D.C.: American Institute of Aeronautics and Astronautics.
[3] U.S. Department of Defense. *System/Subsystem Design Description (SSDD)*, Data Item Description DI–IPSC–81432, December 5, 1994.
[4] Institute of Electrical and Electronics Engineers. *IEEE Recommended Practice for Architectural Description of Software-Intensive Systems*, IEEE STD 1471–2000. New York: Institute of Electrical and Electronics Engineers, 2000.
[5] U.S. Department of Defense. *Software Development and Documentation*, MIL–STD–498, December 5, 1994.
[6] U.S. Department of Defense. *System/Subsystem Specification (SSS)*, Data Item Description (DID) DI–IPSC–81431, December 5, 1994.
[7] International Council on Systems Engineering. *International Council on Systems Engineering (INCOSE) Systems Engineering Handbook*, Version 2.0, July 2000.
[8] Buede, Dennis M. *The Engineering Design of Systems*. New York: Wiley, 2000.
[9] Bergey, J. et al. *Software Architecture Evaluation with ATAM*SM *in the DOD System Acquisition Context*. Carnegie Mellon University/Software Engineering Institute Technical Note CMU/SEI–99–TN012, ADA377450. Pittsburgh: Carnegie Mellon University/Software Engineering Institute, 1999.
[10] Institute of Electrical and Electronics Engineers. *IEEE Recommended Practice for Software Requirements Specification*, IEEE STD 830–1998. New York: Institute of Electrical and Electronics Engineers, 1998.
[11] *Webster's Ninth New Collegiate Dictionary*. Springfield, Massachusetts: Merriam-Webster, Inc., 1988.
[12] U.S. Department of Defense, *DOD Information Technology System Certification and Accreditation Process*, DOD Instruction 5200.40, December 30, 1997.
[13] U.S. Department of Defense, *Department of Defense Information Technology System Certification and Accreditation Process (DITSCAP): Application Manual*, DOD 8510.1–M, July 31, 2000.
[14] National Security Telecommunications and Information Systems Security Committee. *National Information Assurance Certification and Accreditation Process (NIACAP)*, National Security Telecommunications and Information Systems Security Instruction (NTISSI) No. 1000, April 2000.
[15] U.S. Department of the Air Force, Air Force Material Command. *Software Development Capability Evaluation*, AFMC Pamphlet 63–103, vols. 1 and 2, June 15, 1994.
[16] Friedman, George, and Andrew P. Sage. "Case Studies of Systems Engineering and Management in Systems Acquisition," Systems Engineering, volume 7, no. 1, 2004, p. 90.
[17] Green, Connie. *Oracle9i Database Performance Tuning Guide and Reference, Release 2 (9.2)*. Oracle Corporation (Redwood Shores, CA 94065), 2002.
[18] Holdworth, Andrew. *Oracle 9i Database Performance Planning, Release 2 (9.2)*. Oracle Corporation (Redwood Shores, CA 94065), 2002.
[19] Kreitman, Kevin B. *COTS/GOTS Trade Study Report, Aerospace Technical Report Number ATR–2005(5154)–3. The Aerospace Corporation (El Segundo, CA 90245), 17 December 2004.*
[20] Clinger-Cohen Act of 1996 (divisions D and E of U.S. Public Law 104–106).
[21] Federal Enterprise Architecture Program Management Office. *The Technical Reference Model Version 1.1: A Foundation for Government-wide Improvement*, August 2003.

PREPARED STATEMENT OF GLENN A. FINE, INSPECTOR GENERAL, DEPARTMENT OF JUSTICE

INTRODUCTION

Mr. Chairman, Senator Leahy, and Members of the Subcommittee on Commerce, Justice, State and the Judiciary:

I appreciate the opportunity to testify before the Subcommittee as it examines the Federal Bureau of Investigation's (FBI) Trilogy information technology (IT) modernization project. The Trilogy project was designed to upgrade the FBI's IT infrastructure and replace its antiquated case management system with the Virtual Case File (VCF).

Successful implementation of the Trilogy project is essential to modernizing the FBI's inadequate information technology systems. The FBI's systems currently do not permit FBI agents, analysts, and managers to readily access and share case-related information throughout the FBI. Without this capability, the FBI cannot perform its critical missions as efficiently and effectively as it should.

In March 2004, this Subcommittee held a hearing on the status of the Trilogy project, and I testified about the schedule delays and cost increases of the Trilogy project. At that time, I stated that I was skeptical about the FBI's proposed schedule to deploy a fully functional, complete version of the VCF before the end of calendar year 2004. Shortly before the hearing, the Office of the Inspector General (OIG) initiated a follow-up audit to assess the FBI's management of the Trilogy project.

Today the OIG released the results of this follow-up audit. Our audit found that the FBI successfully has completed the Trilogy IT infrastructure upgrades—albeit with delays and significant cost increases. However, the FBI has failed to complete and deploy the VCF, the critical component of Trilogy that was intended to provide the FBI with an effective case management system. The VCF still is not operational after more than 3 years of development and the allocation of $170 million. We found that the VCF either will require substantial additional work or need to be scrapped and replaced by a new system. Moreover, the FBI has not yet provided a realistic timetable or cost estimate for implementing a workable VCF or a successor system.

Our audit also examined the causes for the delays and cost increases in the Trilogy project. Among the problems were poorly defined and slowly evolving design requirements for Trilogy, weak IT investment management practices at the FBI, weaknesses in the way contractors were retained and overseen, the lack of management continuity at the FBI on the Trilogy project, unrealistic scheduling of tasks on Trilogy, and inadequate resolution of issues that warned of problems in Trilogy's development.

In this statement, I describe the OIG's examination of the Trilogy project. The statement is organized into five parts. First, I provide a brief description of prior OIG assessments and testimony about the FBI's IT systems in general and Trilogy in particular. Second, I provide background information on the Trilogy project. Third, I discuss the results of the OIG's recently completed audit regarding Trilogy's cost increases and schedule delays. Fourth, I discuss the OIG's assessment of the causes for the problems in Trilogy's development and implementation. And fifth, as requested by the Subcommittee, I conclude my statement by briefly highlighting several ongoing and recently completed OIG reviews that examine a variety of other issues in the FBI.

PRIOR OIG REVIEWS OF FBI INFORMATION TECHNOLOGY

In a series of reviews over the past several years, the OIG has identified problems in the FBI's IT systems, including outdated infrastructures, fragmented management, ineffective systems, and inadequate training.

For example, a July 1999 OIG review examined the actions of the Campaign Finance Task Force that investigated allegations of improper fundraising practices during the 1996 Presidential campaign. The Task Force relied on the FBI's antiquated case management system, the Automated Case Support (ACS) system, and other FBI databases to obtain information on the individuals and organizations that had become subjects of the investigation. In this review, the OIG noted that deficiencies in the ACS system and the way search results were handled within the FBI resulted in incomplete data being provided to the Task Force.

Another OIG review issued in March 2002 examined how the FBI had failed to turn over to defense attorneys hundreds of FBI documents that should have been disclosed prior to the trials of Timothy McVeigh and Terry Nichols. The OIG again concluded that the FBI's computer systems were antiquated, inefficient, and badly in need of improvement. We found that the ACS could not handle or retrieve documents in a useful, comprehensive, or efficient way, and it did not provide FBI employees with the type of support they need and deserve.

An OIG audit issued in December 2002 examined the FBI's IT investment management practices. This audit concluded that that the FBI had not effectively managed its IT investments because it had failed to: (1) effectively track and oversee the costs and schedules of IT projects; (2) properly establish and effectively use IT investment boards to review projects; (3) inventory the existing IT systems and projects; (4) identify the business needs for each IT project; and (5) use defined processes to select new IT projects. We concluded that the FBI continued to spend hundreds of millions of dollars on IT projects without adequate assurance that the projects would meet their intended goals. Our audit made eight recommendations

with respect to Trilogy, including urging the FBI to establish schedule, cost, technical, and performance baselines and track significant deviations from these baselines.

In a September 2003 audit, the OIG examined the FBI's implementation of the OIG's prior IT-related recommendations. While we found that the FBI had made substantial progress by implementing 93 of 148 total recommendations, we concluded that full implementation of the remaining recommendations was needed to ensure that the FBI's IT program effectively supported the FBI's mission.

As noted above, in March 2004 this Subcommittee held a hearing to examine Information Technology in the FBI, at which the FBI Director testified about the status of the FBI's Trilogy project. At that hearing, the FBI stated that it planned to have "a network with Full Site Capability by late spring" and that it was "closing in on the goal of completion" of the Trilogy project.

The OIG initiated our follow-up audit to assess the FBI's management of the Trilogy project. In December 2004, the OIG completed a draft of this audit report and concluded that the VCF was not operational after more than 3 years of development and the obligation of $170 million, and the FBI did not know when the VCF or a replacement system would be implemented.

Pursuant to our standard practice, in late December 2004 the OIG provided the draft audit report to the FBI for its response. In early January 2005, the FBI publicly acknowledged problems and delays in the development of the VCF. In a written response to our audit report dated January 26, 2005, the FBI acknowledged that the VCF had not met its goals with respect to development of an automated case management system. Nevertheless, the FBI stated that the "VCF project remains the highest IT priority for the FBI."

After receiving the FBI's comments, the OIG completed this audit report and released it today.

I will now provide background on the Trilogy project and the VCF before summarizing the main findings of our audit.

BACKGROUND ON TRILOGY

Trilogy is the largest of the FBI's IT projects. As originally designed, the Trilogy project had three main components: (1) the Information Presentation Component (IPC)—which was intended to upgrade the FBI's hardware and software; (2) Transportation Network Component (TNC)—which was intended to upgrade the FBI's communication networks; and (3) User Applications Component (UAC)—which was intended to replace the FBI's most important investigative applications, including the ACS, the FBI's antiquated case management system. Among its major shortcomings, the ACS does not permit FBI agents, analysts, and managers to readily access and share case-related information throughout the FBI. Without this capability, the FBI cannot efficiently bring together all of the investigative information in the FBI's possession to solve crimes or help prevent future terrorist attacks.

The first two components of Trilogy provide the infrastructure needed to run the FBI's various user applications, while the UAC was intended to upgrade and consolidate the FBI's investigative applications. After the September 11 attacks, the FBI decided to replace the ACS with an entirely new case management system, the VCF.

It is important to note that Trilogy was not intended to replace all 42 of the FBI's investigative applications or the FBI's approximately 160 other non-investigative applications. Rather, Trilogy was intended to lay the foundation so that future enhancements would allow the FBI to achieve a state-of-the-art IT system that integrates all of the agency's investigative and non-investigative applications.

Our audit found that in late April 2004, the FBI completed the first two components of the Trilogy project. The FBI deployed new hardware and software, including 22,251 computer workstations, 3,408 printers, 1,463 scanners, and 475 servers, and it installed new communications networks.

However, as I describe in the next section of this statement, this deployment was not done as quickly as the FBI hoped or expected. Despite the fact that after the September 11 attacks Congress appropriated the FBI an additional $78 million to accelerate deployment of Trilogy's infrastructure components, the FBI completed the two infrastructure components by late April 2004, just before the FBI's original target date of May 2004. Consequently, the FBI missed by some 22 months the completion date for the two infrastructure components under the accelerated schedule funded by Congress. In addition, the total costs for the infrastructure components of Trilogy increased from $238.6 million to $377 million over the course of the project.

And while the infrastructure components are now in place to support improved investigative applications, the FBI still is far from implementing the third component of Trilogy, the VCF.

RESULTS OF OIG AUDIT OF TRILOGY PROJECT

Trilogy Costs

Trilogy originally was planned in 2000 as a 3-year, $380 million project. Over its life, Trilogy has become a $581 million project that has suffered a continuing series of missed completion estimates and associated cost growth.

Initially, in November 2000, Congress appropriated $100.7 million for the first year of the project. In May 2001, the FBI hired DynCorp (which later merged into Computer Sciences Corporation (CSC)) as the contractor for the IPC/TNC infrastructure components of Trilogy. At that time, the scheduled completion date for the Trilogy infrastructure was May 2004. In June 2001, the FBI hired Science Applications International Corporation (SAIC) to develop the user applications component of Trilogy (which became the VCF), with a scheduled completion date of June 2004.

In early 2002, the FBI informed Congress in its *Quarterly Congressional Status Report* that with an additional $70 million in fiscal year 2002 funding, the FBI could accelerate the deployment of Trilogy. Congress supplemented the Trilogy budget with $78 million from the Emergency Supplemental Appropriations Act of January 2002, thereby raising projected costs to $458 million.

In December 2002, the FBI estimated it needed $137.9 million more to complete Trilogy, in addition to the $78 million it had received to accelerate completion of the project. Congress approved a $110.9 million reprogramming of funds that took into account the estimates to complete the IPC/TNC portions of Trilogy, as well as an estimate of the costs to complete the UAC portion. The $110.9 million reprogramming increased the FBI's total available funding for the project to $568.7 million. In addition, $4.3 million for operations and maintenance and $8 million for computer specialist contractor support were added in fiscal year 2003, for a total of $581.1 million—$201 million more than originally estimated.

The following table describes the cost of Trilogy under the original plan and under the current plan:

[In millions of dollars]

Component Area	Original Plan	Current Plan
TNC/IPC	238.6	337.0
UAC	119.2	170.0
Contractor Computer Specialists	n/a	8.0
Integrator	n/a	5.5
Project Management	22.0	32.5
Management Reserve	n/a	28.1
Total	379.8	581.1

Schedule for Trilogy Infrastructure Components

Despite the increased money provided for Trilogy, its implementation has been delayed significantly. Part of the problem we found was that a stable schedule for Trilogy never was firmly established for much of the project's history. Beginning in 2002 the FBI's estimated dates for completing the Trilogy project components began to swing back and forth and were revised repeatedly.

The original completion date for deploying the Trilogy infrastructure (the first two components of Trilogy) was May 2004. After the September 11 attacks, the FBI recognized the urgency of completing the project and moved up the completion date for deploying the Trilogy infrastructure to June 2003. Later, the FBI said the infrastructure would be completed by December 31, 2002. Still later, the FBI informed Congress that with an additional $70 million it could accelerate deployment of Trilogy and complete the two infrastructure components by July 2002 and also deploy the most critical analytical tools in the user applications component.

Yet, the timetable for completing the infrastructure components slipped from July 2002 to October 2002 and then to March 2003. On March 28, 2003, CSC completed a communications network, the Wide Area Network, for Trilogy. The FBI reported that the Wide Area Network, with increased bandwidth and three layers of security, had been deployed to 622 sites. In April 2003, the FBI also reported to Congress that more than 21,000 new desktop computers and nearly 5,000 printers and scanners had been deployed.

In April 2003, the FBI and CSC agreed to a statement of work for the remaining infrastructure components of Trilogy, including servers, upgraded software, e-mail capability, and other computer hardware, with a completion date of October 31, 2003. In August 2003, CSC informed the FBI that the October 2003 completion date would slip another two months to December 2003. In October 2003, CSC and the FBI agreed that the December 2003 date again would slip. In November 2003, the General Services Administration (whose Federal Systems Integration and Management Center, known as FEDSIM, had awarded contracts for Trilogy on behalf of the FBI) formally announced that CSC had failed to meet the deadline for completing work on infrastructure portions of Trilogy that were required to support the VCF user application under development.

On December 4, 2003, CSC signed a commitment letter agreeing to complete the infrastructure components of the Trilogy project by April 30, 2004, for an additional $22.9 million, including an award fee of over $4 million. An award fee is used when the government wants to motivate a contractor with financial incentives. The FBI covered these additional costs by reprogramming funds from other FBI appropriations. In January 2004, the FBI converted the agreement with CSC to a revised statement of work providing for loss of the award fee if the April 30, 2004, deadline was not met. In addition, the revised statement of work provided for cost sharing at a rate of 50 percent for any work remaining after the April 30 deadline.

CSC met the revised deadline of April 30, 2004, for completing the two infrastructure components of Trilogy. As a result, the FBI met the original target set in 2001 for the infrastructure components of Trilogy, but missed the accelerated schedule funded by additional money from Congress by some 22 months.

Schedule for the Virtual Case File

In June 2002, the FBI decided to deploy the VCF user application component of Trilogy in two phases under an accelerated plan: delivery one in December 2003 and delivery two in June 2004. A third delivery eventually was added, also for June 2004. Delivery one was supposed to consist of the initial version of the VCF, which was intended to be a completely new case management system with data migrated from the ACS. The VCF also was intended to serve as the backbone of the FBI's information management systems, replacing paper files with electronic case files. Deliveries two and three under the contract were supposed to consist of enhancements and additional operational capabilities to the VCF.

SAIC provided the first version of the VCF to the FBI in December 2003, in accordance with the accelerated schedule. However, the FBI did not accept that version because the FBI said it was not a functional system and did not meet the FBI's requirements. Deliveries two and three never occurred because of the difficulties experienced in completing the initial version of the VCF. The FBI informed the OIG that these deliveries are not being pursued now given the problems in the first delivery and the FBI's plans to seek a common interagency platform for a case management system (the Federal Investigative Case Management System or FICMS, which is discussed below).

In fact, the FBI has abandoned the intended three VCF deliveries and instead announced a new two-track approach for continuing development of the VCF. Track one, which the FBI refers to as the "Initial Operational Capability," includes a 6-week test of an electronic workflow process scheduled to be completed by March 2005. During this test, the FBI's New Orleans field office and a smaller resident agency office will enter investigative lead and case data into a prototype VCF file system, and this information will be approved electronically and uploaded into the ACS. The FBI intends to obtain user comments on, and assess the performance of, this new workflow system being tested in track one.

However, it is important to make clear that the version of the VCF being tested in track one will not provide the FBI with the case management applications as envisioned throughout the Trilogy project because it represents just one developmental step in the creation of a fully functional investigative case management system. It does not offer full case management capabilities. Rather, it is designed to demonstrate that documents can be approved electronically and uploaded into the existing, obsolete ACS.

The second track, called Full Operational Capability, is intended to reevaluate and update requirements for the next phase of developing a functional case management system to replace ACS. In track two, the FBI plans to identify user activities and processes for creating and approving documents and managing investigative leads, evidence, and cases. As a result of the information gleaned during track two, the FBI is updating and confirming the case management requirements and evaluating whether currently available software can be adapted for a case management system rather than creating a completely new system.

In commenting on the findings in our audit report about the delays in the VCF, the FBI stated that "In many ways, the pace of technological innovation has overtaken our original vision for VCF, and there are now products to suit our purposes that did not exist when Trilogy began." This suggests that the current VCF effort may be obsolete and that the FBI may implement an entirely new system to replace it.

Moreover, our audit found that the FBI still does not have a clear timetable or prospect for completing the project. The VCF case management application was intended to replace the ACS and be the sole system within the FBI that would contain all investigative lead and case file information in a paperless system. Due to the failure to complete the VCF, the FBI continues to lack a modern case management system containing complete and accessible investigative lead and case information. While the FBI cites in its response to our report advances in other FBI IT systems, such as its newly created Investigative Data Warehouse, the VCF case management system would have many features that a Data Warehouse does not. The VCF was intended to be the backbone of the FBI's information systems, replacing the FBI's paper case files with electronic files. Case data in the VCF could be approved electronically, and the electronic files would be available throughout the FBI immediately as entered. Various lead and case information easily could be associated for analysis. The Investigative Data Warehouse, while perhaps a useful tool, does not manage case workflow, does not provide immediate access to case information, and does not substitute for an effective case management system. Consequently, the FBI continues to lack critical tools necessary to maximize the performance of both its criminal investigative and national security missions.

Federal Investigative Case Management System

As a parallel effort to the VCF, the FBI recently has stated that it is pursuing an effort to develop the Federal Investigative Case Management System (FICMS). FBI officials have variously described this effort to the OIG during the course of our audit as a continuation of the VCF, a new investigative case management system to replace the failed VCF, or a "framework" for the future development of an investigative case management system platform.

In its January 26, 2005, formal response to the OIG audit report, however, the FBI stated that the VCF and the FICMS are "two separate, but related projects that will move forward simultaneously. The VCF project remains the highest IT priority for the FBI, and we are developing an implementation plan that will result in deployment of a fully functional investigative case and records management system."

The FBI also stated in its response that it is continuing to pursue the VCF through development of an implementation plan. The FBI hired the Aerospace Corporation to evaluate currently available software products to determine if they meet the FBI's requirements for a case management system. The FBI also asked Aerospace to evaluate the adequacy of the VCF as delivered by SAIC to determine what might be salvaged from that effort.

Yet, the timetable for the FICMS and the VCF still does not appear to be rapid or clear. In conjunction with the OIG's audit, the FBI told the OIG that it hopes to award a contract for FICMS by April 30, 2005. But the FBI has not provided its estimated costs, a revised schedule for completing the VCF, or a schedule for developing a new case management system to replace the VCF through the FICMS effort.

CAUSES OF TRILOGY'S PROBLEMS

We believe the responsibility for ensuring the success of the Trilogy project is shared by several parties: the FBI; the Department of Justice; FEDSIM—the component of GSA that awarded Trilogy contracts on behalf of the FBI; and the two contractors—CSC for the two infrastructure components, and SAIC for the user applications component that became the VCF. These entities, to varying degrees, did not appropriately contract for, manage, monitor, or implement the Trilogy project.

In our view, the main responsibility for the problems with Trilogy rests with the FBI. The FBI acted on a legitimate and urgent need to upgrade its IT infrastructure and replace the antiquated ACS. However, in the FBI's desire to move quickly on the Trilogy project, it engaged FEDSIM to handle the contracting for this very large and complex project without providing or insisting upon: defined requirements, specific milestones, critical decision review points, and penalties for poor contractor performance.

The resulting cost-plus-award-fee contract yielded control to the contactors for developing Trilogy's technical requirements, while leaving the FBI little leverage to direct the project. In essence, the contract terms required paying the contractors regardless of whether they met schedules or were even technically capable of completing such a challenging project.

In addition, the FBI failed to adequately develop and articulate the design requirements at the outset of the project, and consequently the requirements repeatedly changed as the project progressed, with too much contractor control and too little input from FBI management.

In its response to the audit report, the FBI alluded to its lack of control over requirements as a reason for the current VCF problem by stating that "[T]he VCF project suffered in part from runaway scope." The FBI response also stated that to guard against runway scope in the future, "the IT system will be designed, developed, and deployed incrementally against specified and planned parameters."

In addition to the poor choice of contracting method and sketchy requirements, neither the FBI, the Department, nor FEDSIM ensured that adequate schedule, cost, technical, and performance baselines were established to allow the project to be adequately monitored and to identify and rectify schedule slippages or technical problems. Since none of the responsible parties ensured that realistic milestones were established to complete various segments of the project, it was difficult to ensure that the contractors successfully met overall schedule, cost, technical, or performance targets for the project.

In addition, the Department expected the FBI to assume the role of project integrator to ensure all three Trilogy components meshed properly and were on track, even though the FBI lacked this capability or experience. The FBI's ability to manage the Trilogy project, even with the help of contractor personnel, was crippled further by a revolving door of Chief Information Officers (CIOs) and Trilogy project management personnel at the FBI.

A variety of audits by the OIG and the Government Accountability Office, as well as internal FBI reviews, had identified deficiencies in the FBI's management of IT projects, including Trilogy. However, the FBI's corrective action was slow. Only recently has the FBI made substantial progress in its IT investment management processes.

More specifically, in our audit report the OIG detailed the following eight causes for the FBI's problems with the Trilogy project:

—*Poorly defined and slowly evolving design requirements*.—One of the most significant problems with managing the schedule, cost, technical, and performance aspects of the Trilogy project was the lack of a firm understanding of the design requirements by both the FBI and the contractors. Trilogy's design requirements were ill-defined and still evolving as the project progressed. During the initial years of the project, the FBI had no firm design baseline or roadmap for Trilogy. According to one FBI Trilogy project manager, Trilogy's scope grew by about 80 percent since the initiation of the project. Such large changes in the requirements meant that the specific detailed guidance for the project was not established, and as a result a final schedule and cost were not established. In addition, after the September 11 attacks, the FBI recognized that the initial concept of simply modifying the old ACS would not serve the FBI well over the long run. The FBI then created plans for the VCF. Additionally, a need for broadened security requirements due to vulnerabilities identified in the *Hanssen* espionage case affected Trilogy's development. According to one project manager, this recognition of the need to upgrade security caused more problems and delays for the full implementation of the infrastructure component.

—*Contracting weaknesses*.—The FBI's current and former CIOs told the OIG that a primary reason for the schedule and cost problems associated Trilogy was weak statements of work in the contracts. According to FBI IT and contract managers, the cost-plus-award-fee type of contract used for Trilogy did not require specific completion milestones, did not include critical decision review points, and did not provide for penalties if the milestones were not met.

—*IT investment management weaknesses*.—As described in the OIG's December 2002 audit report, *The Federal Bureau of Investigation's Management of Information Technology Investments*, at Trilogy's inception and over much of its life, the FBI's IT Investment Management process was not well-developed. Although our recent audit found that while the FBI had started centralizing its project management structure, appropriate project management was not consistently followed by Trilogy's IT project managers. In essence, the FBI took risks to expedite Trilogy's implementation, and that approach failed because the management practices to oversee Trilogy simply were not in place.

—*Lack of an Enterprise Architecture*.—An Enterprise Architecture provides an organization with a blueprint to more effectively manage its current and future IT infrastructure and applications. The development, maintenance, and implementation of Enterprise Architectures are recognized hallmarks of successful public and private organizations. While the FBI has agreed to develop a comprehensive Enterprise Architecture, this recommendation has not yet been fully

implemented. The FBI has contracted for an Enterprise Architecture to be completed by September 2005. Without a complete Enterprise Architecture, the FBI needed to conduct reverse engineering to identify existing IT capabilities before developing the infrastructure and user applications requirements for the Trilogy project.

—*Lack of management continuity and oversight*.—Turnover in key positions hurt the FBI's ability to manage and oversee the Trilogy project. Since November 2001, 15 different key IT managers have been involved with the Trilogy project, including 5 CIOs or Acting CIOs and 10 individuals serving as project managers for various aspects of Trilogy. This lack of continuity among IT managers contributed to the lack of effective and timely implementation of the Trilogy project. According to contractor personnel who are advising the FBI on Trilogy, the FBI suffered from a lack of engineering expertise, process weaknesses, and decision making by committees instead of knowledgeable individuals.

—*Unrealistic scheduling of tasks*.—Along with the lack of firm milestones in the Trilogy contracts, the scheduled completion dates for individual project components were unrealistic. The unrealistic scheduling of project tasks led to a series of raised expectations followed by frustrations when the completion estimates were missed. According to an FBI official who monitored the development of the Trilogy infrastructure, Computer Sciences Corporation had problems producing an appropriate work schedule given the resources provided for the project. Until the FBI became more active in examining the scheduling of the project, the FBI accepted the project's schedules as presented by the contractor. This acceptance began to shift when the FBI's scheduler worked with the contractor in early 2003 to establish a realistic work schedule for completing the infrastructure components.

—*Lack of adequate project integration*.—Despite the use of two contractors to provide the three major Trilogy project components, the FBI did not retain a professional project integrator to manage contractor interfaces and take responsibility for the overall integrity of the final product until the end of 2003. According to FBI IT managers, FBI officials performed the project integrator function even though they had no experience performing such a role. Although FBI and Department officials stated that the Department required the FBI to perform project integration duties without contractor support, the expertise to adequately perform this function did not exist within the FBI.

—*Inadequate resolution of issues raised in reports on Trilogy*.—Within a matter of months after initiation of the Trilogy project, the FBI recognized significant issues that needed resolution. Internal reports issued by the FBI's Inspection Division, Criminal Justice Information Services Division, and consultants identified a lack of a single project manager, undocumented requirements, and a baseline that was not frozen. Based on internal reports, the FBI was aware of the risks that it faced during the development of the Trilogy project. While FBI management eventually hired a project manager to oversee the project—a recommendation made in all of the reports—the process of defining requirements and baselines for the VCF still continues, more than three years after these internal reports were issued. Because the FBI did not act timely to resolve the findings of these reports, many problems involving project management weaknesses, poorly-defined requirements, and lack of firm targets unnecessarily continued throughout much of the Trilogy project's history.

I believe it is important to note that, despite the troubled history of the Trilogy project, the FBI recently has made some improvements in its management of information technology. One major improvement in the FBI's IT management was the appointment of a new CIO in May 2004 and the consolidation of the FBI's previously fragmented management of IT resources and responsibilities under the Office of the CIO. A significant problem in the FBI's management of IT investments was that all of the FBI divisions with IT investments were not under a single authority and, as a result, had a variety of processes and procedures for developing new systems. Under the reorganization, the CIO is responsible for all of the FBI's IT assets, projects, plans, processes, and budgets.

In December 2004, the Office of the CIO completed an initial version of an IT Strategic Plan, which describes how IT will support the FBI's Strategic Plan and mission goals for the next five years. All IT projects now are required to be consistent with the FBI's Strategic Plan.

The Office of the CIO also has developed an FBI-wide Life Cycle Management Directive to guide FBI personnel on the technical management and engineering practices used to plan, acquire, operate, maintain, and replace IT systems and services. The directive provides detailed guidance to FBI Program and Project Managers and,

if fully and effectively implemented, will help prevent the delays and problems that occurred during the Trilogy project.

As noted above, the FBI also is in the process of creating an Enterprise Architecture by September 2005. The Enterprise Architecture will provide a blueprint to aid the FBI in coordinating and managing its current and future IT infrastructure and systems. The FBI also is working on an IT Portfolio Management Program to list and technically document all of its IT systems. The FBI anticipates that recommendations stemming from its completed IT portfolio will be included in the development of its fiscal year 2007 IT budget.

In commenting on the OIG's Trilogy audit report, the FBI cited a number of other improvements it has begun to make, such as an IT metrics program to identify and measure IT performance, an initiative to standardize and automate IT procurement actions, a Program Management Professional certification training program, a Master IT Policy List to coordinate and control IT policies, standardized technology assessments, and an Information Assurance Program. Further, the FBI told us that VCF track one, or Initial Operating Capability, used the FBI's new IT management approach, including identifying project objectives, requirements, and constraints before proceeding to control gates designed to keep the project on track and to regulate the release of funds. Also, the FBI said it developed a cost-sharing arrangement as part of the renegotiated UAC contract. These initiatives were beyond the scope of our audit, and we could not examine the FBI's claims on these systems. However, they appear to represent progress in the FBI's IT system. But none of them diminish the urgent need for the FBI to fully implement a fully functioning case management system like the VCF to create, organize, share, and analyze case information.

OIG CONCLUSIONS REGARDING TRILOGY PROJECT

In sum, the FBI has made progress with its management of IT and its implementation of the first two phases of Trilogy. Trilogy's infrastructure improvements have been completed, including the delivery of thousands of modern computer workstations and other hardware throughout the FBI. Although the Trilogy infrastructure improvements were characterized by delays and increased costs, the infrastructure now is in place to support improved user applications, including the VCF or its successor case management system, which the FBI recognizes as its top IT priority.

Yet, the VCF effort is incomplete, and the prospects for timely completion remain unclear. After more than 3 years, multiple missed deadlines, and a price tag of $170 million, the FBI still does not have an investigative case management system to replace the antiquated ACS system. Further, we are not confident that the FBI has a firm sense of how much longer and how much more it will cost to develop and deploy a usable system, whether the FBI continues to pursue the VCF system or decides to implement a new case management system.

Finally, we disagree with the FBI's assertion in its response to our draft report that the delays in deploying the VCF and the lack of an adequate case management system do not have national security implications. To the contrary, we believe there is a critical need to replace the ACS to enable FBI agents and analysts to effectively perform the FBI's mission. The archaic ACS 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. While the FBI has made strides in other IT areas—including installing a number of systems to share intelligence information and upload numerous documents into a data warehouse—the continued delays in developing the VCF affects the FBI's ability to carry out its critical missions.

ADDITIONAL OIG REVIEWS IN THE FBI

To conclude this statement, in response to a request from the Subcommittee, I summarize briefly the OIG's ongoing reviews of other priority issues in the FBI. The following are examples of ongoing and recently completed OIG reviews that may be of interest to the Subcommittee.

Ongoing OIG Reviews in the FBI

Terrorist Screening Center.—The OIG is examining the operations of the Terrorist Screening Center to determine how it has managed terrorist-related information to ensure that complete, accurate, and current watch lists are developed and maintained.

Implementation of the Attorney General's Guidelines.—The OIG is reviewing the FBI's compliance with the revised Attorney General Guidelines that govern the use of confidential informants; undercover operations; investigations of general crimes,

racketeering enterprises, and terrorism enterprises; and warrantless monitoring of verbal communications.

Intelligence Analysts.—The OIG is reviewing the FBI's recruitment, selection, training, and staffing of intelligence analysts.

FBI's Handling of the Brandon Mayfield Matter.—The OIG is reviewing the FBI's conduct in connection with the erroneous identification of a fingerprint found on evidence from the March 2004 Madrid train bombing as belonging to Brandon Mayfield, an attorney in Portland, Oregon.

Alleged Mistreatment of Detainees at Military Detention Facilities.—The OIG is examining any involvement of FBI employees in either observing or participating in the alleged abuse of detainees at the military's Guantanamo Bay and Abu Ghraib facilities. In addition, the OIG is reviewing when FBI employees reported the allegations of abuse and how FBI managers handled the employees' reports.

The FBI's Chinese Counterintelligence Program.—At the request of the FBI Director, the OIG is examining the FBI's performance in connection with the handling of Katrina Leung, an asset in the FBI's Chinese counterintelligence program.

The Department's Counterterrorism Task Forces.—The OIG is evaluating the Department's counterterrorism task forces to: (1) determine if they are achieving their stated purposes; (2) evaluate gaps, duplication, and overlap in terrorism coverage; and (3) identify how the performance of each task force is measured.

Implementation of the Communications Assistance for Law Enforcement Act (CALEA).—The OIG is conducting a follow-up audit of the implementation of CALEA, which allows reimbursement to communications carriers for modifications of equipment to allow the capability for lawful electronic surveillance. The FBI has expended more than $500 million under CALEA. The OIG's objectives are to review the progress and impediments to the FBI's implementation of CALEA; review CALEA's costs; and determine how the implementation of CALEA has impacted federal, state, and local law enforcement in their ability to conduct electronic surveillance.

FBI's Reprioritization Efforts.—The OIG is reviewing how the FBI's operational changes resulting from its reorganization and change in priorities after the September 11 attacks have affected other law enforcement agencies.

Recently Completed OIG Reviews in the FBI

The following are some examples of recently completed OIG reviews related to FBI operations:

—*Follow-up Review of the Status of IDENT/IAFIS Integration (December 2004)*.—This OIG review examined ongoing efforts to integrate the federal government's law enforcement and immigration agencies' automated fingerprint identification databases. Fully integrating the automated fingerprint systems operated by the FBI and the DHS, known as IAFIS and IDENT respectively, would allow law enforcement and immigration officers to more easily identify known criminals and known or suspected terrorists trying to enter the United States, as well as identify those already in the United States that they encounter. This latest OIG report is the fourth in four years that monitors the progress of efforts to integrate IAFIS and IDENT.

This OIG report found that while deployment of new IDENT/IAFIS workstations to Border Patrol offices and ports of entry represents a significant accomplishment, full integration of IDENT and IAFIS has yet to be realized. Federal, state, and local law enforcement authorities still do not have complete access to information in the IDENT database. Without such access, the FBI and DHS fingerprint systems are not fully interoperable, and it is more difficult for federal, state, and local law enforcement agencies to identify illegal aliens they encounter.

This OIG report found that the congressional directive to fully integrate the federal government's various fingerprint identification systems has not been accomplished because of high-level policy disagreements among the Departments of Justice, Homeland Security, and State regarding such integration. In addition, the Department and the DHS still have not entered into a memorandum of understanding (MOU) to guide the integration of IAFIS and IDENT. This MOU has not been completed because of fundamental disagreements between the Department and the DHS over the attributes of an interoperable fingerprint system and the number of fingerprints to be taken from individuals by each agency.

—*Effects of the FBI's Reprioritization (September 2004)*.—The OIG reviewed the changes in the FBI's allocation of its personnel resources since the September 11 terrorist attacks. The report provided detailed statistical information regarding changes in the FBI's allocation of resources since 2000. The OIG determined

that the FBI has reallocated resources in accord with its shift in priorities from traditional criminal investigative work to counterterrorism and counterintelligence matters. In addition, the OIG review identified specific field offices most affected by changes in FBI priorities within various investigative areas, such as shifting agent resources from organized crime or health care fraud cases to terrorism investigations. The OIG report recommended that the FBI regularly conduct similar detailed analyses of its agent usage and case openings to provide a data-based view of the status of FBI operations and to assist managers in evaluating the FBI's progress in meeting its goals.

—*Handling of Information Prior to September 11 Terrorist Attacks (July 2004)*.—This classified OIG report, conducted at the request of the FBI Director, examined the FBI's handling of intelligence information prior to the September 11 terrorist attacks. The review focused on the FBI's handling of an electronic communication written by its Phoenix Division in July 2001 regarding extremists attending civil aviation schools in Arizona, the Zacarias Moussaoui investigation, and information related to September 11 terrorists Nawaf al-Hazmi and Khalid al-Mihdhar.

The OIG made 16 recommendations for improving the FBI's intelligence handling and counterterrorism efforts, including recommendations targeted towards the FBI's analytical program. The OIG provided the classified version of this report to the 9/11 Commission and to Congress. In response to requests from members of Congress, the OIG is working with the Department to produce an unclassified version of this report that can be publicly released.

—*Foreign Language Translation Program (July 2004)*.—The OIG audited the FBI's translation of counterterrorism and counterintelligence foreign language materials. The audit found that the FBI did not translate all the counterterrorism and counterintelligence material it collected. The OIG attributed the FBI's backlog of unreviewed material to difficulties in hiring a sufficient number of linguists and limitations in the FBI's translation information technology systems. The review also found problems in the FBI's quality control program for language translations. The report made 18 recommendations for improving the FBI's foreign language translation program.

In response to the OIG report, the FBI stated that it plans to implement a national integrated statistical collection and reporting system for its translation program in fiscal year 2005 that will allow foreign language program management to accurately determine the amount of unreviewed material that needs to be translated. The FBI also plans to increase its digital collection systems' storage capacity so that unreviewed audio material for critical cases is not deleted by the system. In addition, it plans to implement controls to ensure that the forwarding of audio among FBI offices via its secure communications network is accomplished reliably and timely. The FBI further reported that it plans to assess the linguist hiring process, implement measures to reduce the time it takes to bring linguists on board, and strengthen quality control procedures to ensure that translations are accurate and that all pertinent material is being translated.

—*Edmonds Case (June 2004)*.—The OIG examined the FBI's actions in connection with allegations raised by former FBI contract linguist Sibel Edmonds. Edmonds alleged that her concerns about aspects of the FBI translation program were not appropriately handled by the FBI and that her services as a contract linguist were terminated in retaliation for her raising these allegations. The OIG review concluded that many of Edmonds' core allegations relating to the co-worker had some basis in fact and were supported by either documentary evidence or witnesses other than Edmonds. The OIG concluded that the FBI should have investigated Edmonds' allegations more thoroughly. With respect to Edmonds' claim that she was fired for raising these concerns, the OIG concluded that while Edmonds does not fall within the protection of the FBI's whistleblower regulations, Edmonds' allegations were at least a contributing factor in why the FBI terminated her services.

—*DNA Reviews*.—During the past year, the OIG completed three reviews examining various aspects of DNA laboratories or DNA grant programs. In the first review, completed in May 2004, the OIG examined vulnerabilities in the protocols and practices in the FBI's DNA Laboratory. This review was initiated after it was discovered that an examiner in DNA Analysis Unit I failed to perform negative contamination tests. The OIG's review found that certain DNA protocols were vulnerable to undetected, inadvertent, or willful non-compliance by DNA staff, and we made 35 recommendations to address these vulnerabilities. The FBI agreed to amend its protocols to address these recommendations.

In a separate review, the OIG audited several laboratories that participate in the FBI's Combined DNA Index System (CODIS), a national database maintained by the FBI that allows law enforcement agencies to search and exchange DNA information. The OIG's CODIS audits identified concerns with some participants' compliance with quality assurance standards and uploading of unallowable and inaccurate DNA profiles to the national level of CODIS.

In a third review dealing with DNA matters, issued in November 2004, the OIG audited the Office of Justice Programs' DNA backlog reduction grant program. This program provides funding to states for the analysis of DNA samples collected in cases where no suspect has been identified. The audit found that many of the DNA profiles that had been analyzed by the states using grant funding had not been uploaded into the FBI's CODIS system and that grantees were not using the funds on a timely basis to reduce DNA backlogs.

PREPARED STATEMENT OF SENATOR CHARLES GRASSLEY

Chairman Gregg, I want to thank you and the Ranking Member for holding this important hearing on the FBI's Trilogy project and for allowing me to submit a statement for the record. Over the years I have taken a keen interest in making sure that the FBI does the best job that it can. Unfortunately, as Inspector General Fine has testified today, the Trilogy project isn't an example of excellence.

I want to commend General Fine for his report outlining the many problems with the FBI's management of the Trilogy project and it's Virtual Case File. The results of the OIG audit revealed that, although the FBI has completed two of the three components of the Trilogy project, the Virtual Case File (VCF) project has failed to produce a functioning records management system. More importantly, it seems as if the FBI will now actively pursue the development of the Federal Investigative Case Management System (FICMS), but has not provided estimated costs for such a project or a revised schedule for completing the VCF.

The audit has determined that the "main responsibility for the problems with Trilogy rests with the FBI." The fact that changes to the system requirements were made after the project had been initiated, that contracts were not monitored and that project management decisions were made by committees instead of experts with a working knowledge of these systems, are all indicative of a plan that had failed before it even got off the ground. The absence of an Enterprise Architecture and lack of proper scrutiny over the various contracts leads one to believe that funds for this project were requested from Congress before a rational and pragmatic review of the potential problems were examined.

Today's OIG audit is another verse of the same song. On several occasions in the last few years, the IG has had opportunity to examine the FBI's automated case support and its IT systems. They have highlighted the flaws and deficiencies and made recommendations. As the IG noted in September 2003, the FBI implemented many of the IG's recommendations, but not all of them. Had the FBI fully embraced these recommendations the Trilogy project might have been in a different place today. In fact one of the problems we see today was noted in December of 2002. At that time, the IG concluded that the FBI was spending hundreds of millions of dollars on IT projects without adequate assurance that the projects would meet their intended goals. Apparently, not much has changed.

This is particularly troubling, in light of the dire need for a case management system that works. I agree with the IG's assessment that "there is a critical need to replace the ACS to enable FBI agents and analysts to effectively perform the FBI's mission." Fighting terrorism is the FBI's main job and not having an adequate ACS hinders their effort. The FBI asserts that the failure of the VCF will not impact on national security, but frankly, I'd rather not take the chance. Securing the homeland is far too important of a task to not have the best tools available.

After having spent $580 million on the Trilogy project, including $171 million on the Virtual Case File, one would think that the FBI didn't just have the best tools, but they have all of the tools. Unfortunately, the taxpayers $171 million was squandered on a project that doesn't meet the FBI's needs. Additionally, the fact that the FBI has been set back three years in planning their critical infrastructure, necessitates a well thought-out and managed solution. I hope that from this failure the FBI can gain some insights and build a learning curve that will help them as they look for a another system.

To that end, I would recommend that the FBI explore the case management programs already utilized by other federal government agencies, before attempting to spearhead a Federal Investigative Case Management System. It is quite possible

that a program currently in use by the federal government could be adapted to suit the needs of the FBI case management program.

Chairman Gregg, I again want to thank you for giving me the opportunity to weigh in on this critical topic. General Fine, thank you for your thorough and insightful report and testimony. I really do want the FBI to be the best they can be at protecting America's citizens, and that's why this report and hearing are so very important. The FBI must learn from its mistakes. To not do so could lead to an even greater waste of taxpayers' dollars and increased risk to national security.

ADDITIONAL COMMITTEE QUESTIONS

Senator GREGG. But I am going to have to recess this hearing and we are going to have to come back and reschedule the balance at another date. I think the time that the Director has given us has been exceptional and it might have been a little longer than people had expected, but we appreciate his courtesy.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing:]

QUESTIONS SUBMITTED BY SENATOR PATRICK J. LEAHY

VIRTUAL CASE FILE

Question. There is a field test of the VCF Initial Operating Capability currently underway in the New Orleans field office. (A) When will that test be completed? Who will assess the results of that test and what criteria will be applied? (B) What are the Federal Bureau of Investigations (FBI's) plans for "VCF-lite?" Does it expect to use this software in the future?

Answer. The deployment of the Virtual Case File (VCF) Initial Operating Capability (IOC) as a pilot to the New Orleans Field Office, the Baton Rouge Resident Agency, the Criminal Investigative Division's Drug Unit, and the User Advocate Unit provides the opportunity to refine workflow business processes, verify workflow requirements, quantify workflow efficiency improvements, develop workflow-related system deployment processes, and develop workflow-related training processes. During the pilot, metrics are being collected to quantify the above goals and assess user satisfaction. At the end of the pilot activities, the FBI will better understand the opportunities an electronic workflow capability provides for improving the efficiency of document-related business processes and the challenges involved in deploying a web-based workflow application across the workforce. Questions the FBI hopes to answer include:

—Will the automation of workflow reduce investigation time?
—Will the application track documents throughout their existence?
—What is the impact of the automated workflow on the FBI workforce?
—What is the best way to train FBI employees on new technology tools and capabilities?
—Is the user interface acceptable to the users and does it enhance their ability to do their work efficiently and effectively?
—What is needed to implement more effective security controls to ensure seamless access to data and information sharing?
—Will the interface between the Automated Case Support (ACS) system and the VCF IOC be adequate for future system integration efforts, including "flash cut-over" strategies?

The pilot was completed in late spring of 2005, metrics are being analyzed and reported. The FBI has tasked Mitretek Systems to perform the assessment to determine what future use of the application is appropriate. The results of this pilot, along with the conclusions drawn by the Office of the Chief Information Officer (OCIO), will be shared with The RAND Corporation as well as our oversight partners, including the Congress, Office of Management and Budget (OMB), and Government Accountability Office (GAO).

The IOC was developed in two increments: the initial IOC and the incremental "IOC Plus." The incremental IOC Plus consists of a few additional features that were identified during the beta test as significantly enhancing the usability of the IOC and capable of development and testing for a minimum additional cost. Based on feedback from users during the pilot, the FBI will determine the value and cost of deploying IOC Plus field-wide. Such a deployment would provide a stop-gap capability while the Full Operating Capability solution is being developed. The FBI has

prepared a cost estimate for deploying IOC Plus field-wide and associated operations for a 12-month period. These costs will be analyzed along with the perceived benefit of such a deployment to the user community, resulting in a recommendation of whether to deploy IOC Plus field-wide.

Aspects of the pilot software will be used in the future. In particular, the Web ACS capabilities integrated into the pilot are being further developed and will provide users increased access to ACS data. In addition, the software implementing the workflow aspect of the pilot is under evaluation for longer term, future use. There are no plans for a "VCF-lite."

Question. You told this subcommittee on March 23, 2004, that in the wake of the 9/11 attacks, you evaluated whether to develop VCF or purchase a commercial off-the-shelf product. You stated: "I have had a number of persons outside the bureau look at the decision to develop our own, persons—I call them the gray-beards—who are from a number of private concerns who would look at the choice we made and the product we've come up with. And I think the reviews are very good for the product we've come up with." Did these "gray-beards" from private concerns produce written or otherwise formal assessments of whether the FBI should develop its own product or buy off-the-shelf? If so, please provide those. If not, why did the FBI chose to rely on an informal assessment rather a formal report like the one recently prepared by Aerospace? Couldn't the FBI have benefited by contracting for a formal report on off-the-shelf alternatives much earlier?

Answer. Two groups of "gray beards" reviewed Trilogy and/or VCF. A panel from the National Academy of Science (NAS), led by Jim McGrotty, looked at Trilogy first in September 2002, and then again during late 2003 and early 2004. The initial NAS effort in September 2002 consisted of two days of briefings, after which the panel provided an oral assessment to the Director and others. No formal written report was issued. The purpose of this review was to give the Director a "pulse-check" on how Trilogy was proceeding. The second NAS review resulted in a written report, issued in May 2004, and was followed by an addendum in June 2004, that focused on changes made by Zalmai Azmi, after his appointment as the FBI's Chief Information Officer (CIO) (which were not considered in the initial report). The NAS was not asked to assess commercial off-the-shelf (COTS) products, although some panel members believed, from the discussion of requirements presented, that COTS products might meet FBI requirements.

The second group of "gray beards" is the Director's Science and Technology Advisory Board, led by Art Money. This Board has been briefed on Trilogy, VCF, and the FBI's information technology (IT) effort in general since it first began meeting in October 2003. At the request of former FBI Executive Assistant Director Wilson Lowery, members of the Board met in June 2004, specifically to review and comment on the VCF Corrective Action Plan, including the identification of any inconsistencies or gaps in the remediation plan. After a series of briefings during the day, the Board members met with the Director to provide an oral assessment of the plan and other suggestions. Since then, VCF, Enterprise Architecture (EA), and IT have been regular agenda items on the Science Board's agenda, and the program managers have updated the board members. Again, the Board was not asked to assess COTS, but they also suggested that COTS could satisfy most of the FBI's requirements and encouraged the FBI to explore that option.

Question. On July 16, 2002, Sherry Higgins, your then-Project Management Executive, testified before the Senate Judiciary Subcommittee on Administrative Oversight that the FBI was using an industry-standard process—Joint Application Development—to "define and prioritize" its requirements. The subcommittee was also told this was a new way of doing business: bringing together users, designers, and future systems operators to define and prioritize requirements. Why was this process not effective in producing a concrete and final list of VCF requirements that SAIC could use to build VCF?

Answer. The Joint Application Development (JAD) sessions resulted in user-need and requirements statements reflecting the capabilities users desired in the final system. These statements were, however, not prioritized and, in some important aspects, insufficiently detailed (this was particularly true of the requirements related to users' access to the system's functions and data and to the requirements defining the system's administrative functions). As a result, the requirements were accurate and consistent, but they were not complete in all areas. In addition, they did not reflect the constraints imposed by the system's conceptual design or current infrastructure, since the process by which requirements were defined was implemented after the Science Application International Corporation (SAIC) had already developed the conceptual design and the infrastructure framework. The SAIC attempted to use these user-need and requirements statements to define a set of requirements that were consistent with a vision of how to build the system, but were unsuccessful

because the JAD lacked sufficiently detailed requirements regarding security, records management, and the intelligence mission to complete the new system and application architecture.

Question. At the hearing on February 3, you described problems leading to a failed VCF effort, including that the FBI "lacked skill sets in our personnel, such as qualified software engineering, program management and contract management." You also stated that the FBI responded to these deficiencies by outsourcing the contract management and technology development. The Federal Systems Integration Management (FEDSIM) is acting as the contracting office on behalf of the FBI, and Mitretek Systems provides program management, systems engineering and technical advisory services. SAIC has been responsible for delivering VCF.

Has the FBI or an outside entity evaluated the extent to which it should have such capabilities within its own staff, and if so, what is the result of that assessment?

Answer. In 2003, a distinguished group under the NAS conducted an in-depth study of the Trilogy program including, in particular, VCF. The NAS determined that, while the FBI had some good IT people, it fell short of the kind of expertise needed to manage large IT acquisitions, not only from the program management perspective, but also from an engineering perspective.

The FBI recognized these shortcomings and created the Office of the Chief Technology Officer (CTO) in June 2004, to strengthen engineering and computer science especially as it relates to the development of new technology. Currently, that office includes 10 software/system engineers and is in the process of selecting an additional 10, which will be a combination of new employees and transfers from other parts of the FBI. At the same time, the CTO is strengthening software, system, and data engineering at the Bureau by hiring contractors to work on establishing "to be" technical and data reference models for the enterprise, participating in project and critical design reviews, and base-lining the FBI's capabilities from a systems engineering perspective. The FBI plans to request additional government software and systems engineers in the future to bolster its resource pool for dealing with complex and critical information technology projects.

Additionally, the FBI's Office of IT Program Management (OIPM) has taken several steps to strengthen program management skills as they relate to IT programs and projects. In addition to recruiting several experienced program managers to fill key IT management positions within the OIPM, the FBI has implemented a training initiative through which employees can be certified as Program Management Professionals. Since September 2004, 30 employees have been trained and two additional classes, with an additional 50 students, are underway.

On March 4, 2005, the FBI became a member of the Program Management Institute (PMI), and enrolled 20 employees in this professional organization. In addition, these individuals joined the Washington, D.C. PMI Chapter and the government special interest group. This allows FBI program managers to remain updated on the latest information from PMI, attend project meetings, and participate in the government-specific interest group.

Question. What adjustments did the FBI make to its own internal personnel to ensure proper oversight of, and effective communication with, SAIC, FEDSIM, Mitretek and other entities performing functions related to VCF?

Answer. While the FBI did take steps to improve internal oversight of the VCF project, in retrospect the steps were not adequate to ensure proper oversight. Steps taken included, but were not limited to, the following: (1) a communication plan between the FBI User Team and SAIC where FBI User Team members were integrated into SAIC's environment for project support; (2) an interim Award Fee feedback plan instituted by the FBI and the Federal Systems Integration Management (FEDSIM) Center to provide SAIC more frequent performance analysis; (3) monthly In-Progress Review (IPR) briefings provided by SAIC to FEDSIM and the FBI; and (4) weekly Program Management Office (PMO) meetings, attended by SAIC, FEDSIM, and the FBI.

Once it became apparent that SAIC was having difficulties, the PMO co-located FBI and Mitretek Systems personnel at SAIC. Mitretek was asked by the FBI to provide additional resources to help resolve issues. In addition to attending ad hoc meetings as issues arose, Mitretek Systems developed a User's Guide and a series of white papers to assist SAIC in understanding the FBI's needs and requirements in areas not covered in detail in the system and software requirements. The white papers addressed such topics as: access control concepts, authorized users, delegated functions identified in the Systems Requirements Document, lead routing table concepts, package assumptions rules and roles, silent hits, User Application Component client server communications link bandwidths, logging, and data models.

In the first quarter of 2004, an independent FBI Special Technologies and Applications Section technical team provided an architectural evaluation, identifying risks and deficiencies previously suspected, but not confirmed, to the PMO. This new risk information, in addition to SAIC's past performance on this project, became an important component in the FBI's assessment of SAIC's ability to respond to the challenges of completing VCF delivery 1.

Question. Prior oversight reports have found that the bureau has had trouble managing its information technology contractors and that these problems contributed in part to cost, schedule, and performance shortfalls on system modernization projects such as Trilogy/Virtual Case File. For example, in December 2002, the Inspector General reported that the bureau was not implementing cost, schedule, and technical baselines to monitor its contractor's progress on the Trilogy project. In addition, in May 2004, the National Research Council reported that the bureau needed more control over its Trilogy/Virtual Case File contracts, including more frequent use of contractor progress reviews, performance metrics, and specific milestone delivery dates. What has the FBI done to strengthen its ability to effectively manage its contractors and minimize the risk that the bureau will experience cost, schedule, and performance shortfalls on future IT projects?

Answer. In May 2004, Director Mueller announced the appointment of Mr. Zalmai Azmi as the FBI CIO. Mr. Azmi is responsible for the FBI's overall information technology efforts, including developing the FBI's IT strategic plan and operating budget; developing and maintaining the FBI's technology assets; and providing technical direction for the re-engineering of FBI business processes. Mr. Azmi was given the authority for enterprise-wide IT budget control/consolidation. The CIO and Chief Financial Officer (CFO) work closely together on all IT financial and budget matters (including the IT budgets in all FBI divisions). The CIO and CFO instituted an acquisition process that required all IT investments to be reviewed by CIO and CFO staff. Almost 1,000 acquisitions were reviewed and approved in the last 2 quarters of fiscal year 2004. The risks associated with cost, schedule, and contract performance are also reduced by the FBI's close coordination with the Department of Justice (DOJ) CIO; the FBI and DOJ CIOs meet regularly to discuss status and address issues related to the FBI's major IT investments.

The CIO centralized the IT business of the FBI, mostly in an organizational structure under his office with a few specialized applications organizationally separate but reporting through him (e.g., the Criminal Justice Information Systems Division in West Virginia) under the Life Cycle Management Directive (LCMD). The LCMD, which fundamentally changes how IT projects are managed in the Bureau, governs how IT projects are managed from "cradle to grave" and is consistent with industry and other government agency best practices. The LCMD guides FBI personnel on the technical management and engineering practices used to plan, acquire, operate, maintain, and replace IT systems and services. All IT projects and programs will be required to undergo rigorous project and executive level "control gate" reviews for each stage, from inception through disposal. There are seven gates, nine phases, and 14 key supporting processes in the LCMD. These reviews are the mechanism for management control and direction, decision-making, coordination, and confirmation of successful performance.

The FBI's CIO has established a system of review boards through which the IT business of the FBI is conducted.

—The IT Advisory Board ensures new technologies are incorporated into FBI operations and business practices, ensures decision makers prioritize operational technology needs for future development, minimizes duplicate technology business practices to better optimize resources, and resolves conflicts involving IT issues among FBI Headquarters divisions.

—The EA Board ensures IT systems comply with EA requirements, the supporting system concept, critical design, and disposal reviews.

—The IT Policy Review Board provides guidance and direction on IT policy matters, resolves issues, and develops new policies.

—The Technical Review Board ensures IT systems comply with technical requirements, leads critical design, and supports deployment readiness and system test reviews.

—The Change Management Board manages IT infrastructure changes, leading deployment readiness, system test readiness, operational acceptance, and disposal reviews.

—The Investment Management Project Review Board ensures IT systems acquisitions are aligned with IT policy, strategic plans, and investment management/portfolio management requirements. It leads system concept and acquisition plan reviews.

These Boards have defined roles/responsibilities within the structured framework of the LCMD and operate pursuant to established charters and procedures. The LCMD applies to all solution providers, including contractors. In addition, contract management is enhanced at the Departmental level by the work of the Department Executive Review Board (DERB), which oversees DOJ's major IT investments, including those led by the FBI. The DERB operates as part of DOJ's Information Technology Investment Management process to provide oversight at the highest level.

Through a newly instituted IT Investment Management process, the CIO is establishing control and management of IT project budgeting, working with the CFO in the budget formulation process during the fiscal year 2006 budget cycle (the Finance Division has asked the CIO to provide an addendum to the fiscal year 2007 budget request targeting IT requirements). In addition, the OCIO has increased the oversight of IT projects and programs through the development of IT standard system/project definitions; identification of the FBI IT portfolio of systems, applications, programs, and projects; release of the FBI IT Master Project/Programs list; promulgation to all FBI divisions of the LCMD; and purchase of an Enterprise Portfolio Management tool and a Project Portfolio Management tool.

Oversight of IT projects begins with establishing baselines for each project. In June 2004, it was mandated that all new projects produce and maintain resource-driven MS Project 2002 schedules. These schedules are subject to periodic (weekly, monthly, and/or at LCMD gates, depending on the project) review and analysis. All pre-existing projects will be required to produce and maintain project schedules, which are subject to review and analysis at each of the remaining LCMD gate reviews. DOJ has announced their implementation of a congressional mandate that all projects of a certain size are required to provide American National Standards Institute Earned Value Management Systems data. The Earned Value Management (EVM) methodology is a project (investment) management process that effectively integrates the investment scope of work with schedule and cost elements for optimum investment planning and control. The OCIO is in the process of reporting EVM data to DOJ in compliance with this mandate.

Question. When SAIC submitted invoices as it spent taxpayer's money, what were the FBI's procedures for evaluating: (a) whether those expenditures were permissible under its contract; (b) whether they were producing the necessary result; and (c) whether the timing of those expenses put SAIC on track for timely delivery? Why did those procedures fail to identify at an earlier date that SAIC would not be able to deliver the expected results on the due date, and what changes have been put in place to manage future contracts?

Answer. In a large system development project such as VCF, the key is the development of a base-lined, resource-loaded network addressing both schedule and resources. Tracking progress against this resource-loaded network reveals whether the money is being spent according to the plan and the development is on track. While SAIC had a resource-loaded network, it was not sufficiently milestone driven to expose the difficulty they were having completing the system development. Even with this weakness, the FBI was aware of the project status. Over the past year, the FBI has met with DOJ officials and with House and Senate Committee Members and/or their staffs to address issues regarding the VCF and Trilogy programs.

The FBI is acutely aware of these deficiencies and has taken proactive steps to ensure that they do not recur. As noted above, all projects will be managed in accordance with the Life Cycle Management Directive. Earned Value Management (EVM) reporting requirements will be mandated on projects of a specified size and dollar threshold. A work breakdown structure and a detailed, integrated, event-driven schedule will be developed and maintained for each project. Project status reporting will be accomplished at both the project and enterprise levels. Project Management Reviews will be conducted at the project level, and "control gate" reviews will be conducted at the enterprise level. Appropriately designated boards will oversee projects and, through the recent deployment of Worklenz software, all oversight entities will have the same view into a project's progress. The oversight process will also be enhanced by the monthly entry of key budget and milestone data for all DOJ IT projects, including FBI IT projects, into DOJ's IT Dashboard, which will allow the FBI's and DOJ's CIOs to view status, EVM metrics, and major developments affecting progress.

While clearly VCF does not provide the capabilities the FBI sought, the "lessons learned" from the VCF project management were beneficial. As noted above, the FBI has developed the LCMD to impose structure and process in system development, and the VCF IOC was executed using this new approach to IT management. Project objectives, requirements, and constraints were clearly identified before proceeding to each control gate, and "go/no go" criteria were used at major milestones to control

the release of funding and to keep the project focused. In addition, a cost-sharing arrangement was established as part of the renegotiated User Applications Component contract, and adherence to defined management processes was mandated. As a result, the VCF IOC development and deployment was completed on schedule and within budget.

Question. At the hearing, you indicated that the FBI has deferred to DOJ for consideration of whether the FBI can recoup any funds from SAIC, and if so, how much and on what basis. When was this issue deferred for consideration and when do you expect to receive an answer? Will you inform the Committee immediately upon receipt of this assessment?

Answer. The FBI referred this matter to DOJ's Civil Division on February 2, 2005. The FBI asked the Civil Division to "begin to analyze the facts to assist us in determining the appropriate course of action" concerning the possible recovery of funds from SAIC. The FBI is continuing to work with the Civil Division and the General Services Administration to resolve this matter and determine what future action, if any, will be taken. At this point, it is not known when a final determination will be made. The FBI will inform the Committee when such a determination is made.

Question. The FBI's response to the Inspector General's draft report indicated that the FBI established its baseline Enterprise Architecture (EA) in 2004 and is in the process of developing a target EA in September 2005. What is the status and progress of the bureau's efforts to develop and implement an effective and complete EA that can be used to effectively guide and constrain its IT investments, and will it be complete by September 2005? Does it make sense to continue to pursue VCF, or even the Federal Investigative Case Management System (FICMS), before this EA is complete?

Answer. Since the award of a contract for EA support on March 21, 2004, the FBI has applied a focused, concentrated, and elevated effort. For example, a revised EA Program Plan was completed and signed by the CIO on July 2, 2004. EA development efforts and products are being reviewed approximately every other month by the Director's Science and Technology Advisory Board, an external group of senior scientists and technology experts. Both completed and in-progress EA products are also reviewed by the EA Board (EAB), which includes Deputy Assistant Directors from FBI Headquarters Divisions. The EA principles and the Integrated EA Base were completed and approved by the EAB and the CIO on December 9, 2004. The Integrated EA Base Line, which was approved by the FBI Director on December 21, 2004, contains the following information.

—Business Architecture—36 stakeholders, 42 functions, 223 sub-functions.
—Data Architecture—identified 8 data areas and 65 data classes.
—Applications Architecture—includes the Master IT Systems List with an inventory of over 500 FBI systems, applications, networks, and databases.
—Technology Architecture—includes the FBI IT Master Products List with over 800 COTS and Government off-the-shelf products.

The CIO has added both in-house personnel and contractors to ensure completion of the target, or "To Be," EA by May 2005. The initial phase, referred to as the "interim To Be architecture," addresses the target architecture and the Integrated Baseline Architecture, focusing on current projects and interoperability within the current technology environment. Any project that is being developed with incremental capabilities will need to be aware of the architectural impact of projects in-progress to address integration issues. Phase I of the target architecture identifies the mission requirements being supported by the FBI projects identified for fiscal year 2005 and 2006, including VCF, and the EA team is working with the personnel responsible for the VCF to ensure that its architectural issues are addressed. The interim target architecture includes mapping to the reference models identified in the Federal EA, tailored for the FBI environment to provide architectural support for projects under development. The intent is to create an optimum architecture environment for the implementation of projects that enhance the FBI's technical environment so the FBI is in an optimum position to support the VCF effort.

Question. Mr. Azmi testified at the hearing that the FBI now has a list of requirements for VCF and has mapped these requirements "through a federal enterprise architecture framework," that these have been broken down into phases, and that another independent contractor is assessing the cost of implementing those phases and will have a report by mid-February. What is the relationship between this "federal enterprise architecture framework" and the FBI's efforts to develop its own EA by 2005?

Answer. The Federal EA Framework (FEAF) that was initially established in fiscal year 2000 has been evolving with the development of OMB's five reference models. For example, the original FEAF did not contain any framework support for se-

curity. Additionally, OMB and GAO recognized that focusing on specific organizations' applications retained the dependencies or bottlenecks within these organizations. Therefore, OMB replaced that approach with one that employs the concept of service components independent of an application's implementation. Some of the reference models, including the Security reference model, are still under development. The OMB approach is to include in the reference models a master list of all possible elements, so that an organization can develop its own reference model by selecting the elements appropriate to that organization. The FBI is using the OMB reference models to complete its EA to the extent possible, adding additional features or framework elements, such as security services and features, as appropriate. The FBI target model also uses the reference models, but depicts the future environment the FBI expects to need to meet mission goals. The difference between the baseline EA and the target EA represents the gap that must be bridged to achieve the target EA.

Question. Is the list of requirements referenced in the hearing the final list of requirements against which VCF will be built, or will there be additional changes to the requirements list, perhaps when the FBI's own EA is complete in 2005?

Answer. The FBI contracted with BAE Systems to review and revalidate users requirements because the mission of the FBI has evolved, presenting new requirements for information and intelligence sharing among different entities. This review is still in progress. To ensure future IT systems do not expand beyond their functional level, IT systems will be designed, developed, and deployed incrementally against specified and planned parameters.

Question. Which independent contractor is developing a cost estimate, and will you provide the cost-estimate report to Congress upon receipt? Does it make sense to solicit cost estimates at this time given the potential flux in the VCF requirements?

Answer. Two Independent Government Cost Estimates (IGCEs) are being developed, one by Mitretek Systems and one by Aerospace. Aerospace is a Federally Funded Research and Development Corporation and is Congressionally chartered to provide this kind of analysis. An IGCE is based on a set of assumptions addressing the concept and its development, operations, and maintenance. Given the current fluidity in the concept's development, these estimates will need to be revisited when the final concept has been defined.

Due to the rigor and time associated with developing an IGCE, the FBI decided to begin preparing the estimates and factor in time for later updates, rather than waiting until everything is known to begin to prepare the estimates.

The FBI would be pleased to brief the Subcommittee on our progress in this area.

Question. The OIG Report indicates that the FBI discontinued its pursuit of certain enhancements and additional operational capabilities to VCF in part because the VCF Delivery 1 did not meet its expectations, and also because the FBI plans to pursue the Federal Investigative Case Management System (FICMS). The OIG Report also indicated that the FBI is serving as the executive agent of the process to award a contract for FICMS by April 2005. The FBI's response to the OIG's draft audit described FICMS as a "blueprint" and stated that VCF and FICMS "are on parallel tracks that will eventually converge." What will this "blueprint" entail and who designed it?

Answer. The Federal Investigative Case Management Solutions (FICMS) initiative, part of OMB's Case Management Line of Business, is a framework that provides guidance for participating agencies designing and developing investigative case management systems. FICMS ensures, where appropriate, the establishment and reusability of common IT solutions and promotes the inter-agency compatibility and system interoperability needed to facilitate information sharing across the federal investigative and law enforcement landscape. Investigative agencies share core business functions but also have unique needs that drive agency-specific system requirements. The FICMS framework uses a Service Oriented Architecture approach, which allows agencies the flexibility to implement a common, core solution and build specific functional modules that plug into the common solution to meet unique agency needs. Accordingly, investigative agencies will procure commercially available solutions where appropriate, then implement these solutions to address specific activities such as investigative workflow management, records management, and data analysis. These agency-specific systems will follow the broad FICMS blueprint so that data can flow easily and securely between agencies. The FBI is planning to implement the first investigative case management system as part of the FICMS framework, and is collaborating with DOJ and the Department of Homeland Security (DHS) to maximize the system's use by other investigative agencies, thus preventing costly investments in duplicate IT case management systems. OMB selected

DOJ to lead this effort, and the FBI was designated as DOJ's Executive Agent for FICMS development.

Question. What impact has the development of FICMS had on the FBI's view of, or plans for, VCF? What does it mean that VCF and FICMS "are on parallel tracks" and "will eventually converge?"

Answer. The FBI is continuing to move forward to develop and deploy a case management system. At the same time, the lessons learned through VCF will be used to help develop the FICMS, a broad blueprint for federal investigative case management systems being led by DOJ. The FBI will use the FICMS framework to develop an investigative case management system that will not only meets the Bureau's specific needs, but will also provide a blueprint for other federal investigative agencies implementing case management systems. The use of this common FICMS framework will permit more seamless information sharing.

Question. Will FICMS benefit from the 3-years and $170 million devoted to the VCF effort, and if so, in what ways?

Answer. Yes, the lessons the FBI has learned in its efforts to develop VCF will help in developing the FICMS, particularly in the areas of contract management, project management, the development and implementation of policies and procedures, modular development and deployment, data security, records management, and training. For example, the FBI learned that it should not attempt a "flash cutover" (i.e., a full implementation of a system in which all functionality is brought online initially) when migrating from the legacy system to the new system. Instead, the FBI should develop and incrementally deploy capabilities in phases. Also, business process requirements captured through the JAD sessions will be used in the development of the FICMS requirements. The electronic interfaces developed between the legacy ACS application and VCF IOC are being evaluated for possible reuse. The metrics and lessons learned from the New Orleans Pilot, which are currently being compiled, will also influence the development of FICMS.

Question. How will FICMS relate to the FBI's enterprise architecture? What steps has the FBI taken to ensure that these efforts will interrelate, rather than conflict?

Answer. The FBI is using the FEAF as the basis for the development of the FBI EA. OMB requires that federal agencies use the FEAF, which will ensure interoperability between systems and easy information sharing. The FBI will use the Service Reference Model of the FEAF as the FICMS framework for delivering services in a phased approach to participating federal agencies based on their determined priority. Each phase will deliver capabilities independently.

Question. Is there a defined list of requirements for FICMS, such that soliciting contracts for FICMS in April will be an efficient and productive process?

Answer. The goal of this program is to ensure compatibility between all systems used by the various entities in DOJ and DHS. In order to ensure that all technology requirements will be included in the system's overarching framework, the FBI sent system requirements to DOJ and DHS for review. DOJ and DHS responded by providing additional requirements that are necessary for their operations. Based on this input, the FBI created a larger set of requirements encompassing the needs of the FBI, DOJ, and DHS. This approach ensures that all components' investigative needs be addressed by the framework.

Question. Besides DHS, what other departments and agencies will FICMS serve?

Answer. FICMS will serve as a framework for investigative information technology systems used by the FBI, DOJ (including DOJ components), and DHS.

Question. At the hearing, you stated that the FBI "did not have a complete set of defined VCF requirements when the original contract was signed in June 2001, and we did not have a finalized set until the summer of 2002." In addition, FBI CIO, Zal Azmi testified that "we have completed our requirements. We have a requirements document for a case management system that our users, our agents, our analysts want and the FBI. We have mapped those requirements to our services that are guidelines by the federal enterprise architecture framework." However, the Inspector General's recent audit stated that "the process of defining requirements and baselines for the VCF still continues," and recommends that the FBI "freeze the critical design requirements for the case management system before initiating a new contract." Can you reconcile these statements? Are the requirements for VCF now frozen and final until a case management system is delivered? How can the VCF requirements be final when the FBI does not have a complete EA? When the requirements are finalized, will an outside expert evaluate the list of requirements, and if so, who and when?

Answer. The OIG report was written in late 2004. Since that time, the FBI has made significant progress in documenting the requirements and Concept of Operations (CONOPS) for an enterprise-wide case management capability. In January 2005, the FBI completed the System Requirements Specifications (SRS) and System

CONOPS. The SRS have been revised based on feedback provided through a review process, and will be finalized at the end of the review/revision process. The CONOPS is also undergoing that review/revision process. A System Requirements Review for completeness is also ongoing and, after all inputs are incorporated, the final set of system requirements will include approval by each of the Lines of Business owners. The systems engineering team is working with the EA team to ensure system requirements meet EA objectives. Additionally, requirements will be put under formal Configuration Management control. Requirements will be base-lined at contract award and, after contract award, changes or proposed changes to the system or requested functionality will be managed in accordance with the Configuration Management Key Support Process of the Life Cycle Management Directive. The requirements have additionally been presented to the Director's Science and Technology Board.

Question. You testified at the hearing that agents will have "a basic case management system" in their hands within a year. What specifically will a "basic case management system" entail and will its delivery complete the VCF project? If for some reason developments threaten to delay delivery beyond 2005, will you inform this subcommittee immediately?

Answer. The FBI has expended significant time and effort since the hearing confirming requirements for a new case management system, as well as developing a procurement strategy that will take advantage of off-the-shelf products. At this time the FBI envisions the deployment of the new case management system in four phases, each of which will provide discrete aspects of the new case management system. The first phase should be completed 9 to 12 months after contract award, which is expected in the summer of 2005. However, we would not expect a "basic case management system" to be in place until the completion of phase 2, which will not be until 2006. Phases 3 and 4 will add additional capabilities to the system.

Question. In your testimony, you stated that within 6 to 8 weeks you would have an assessment of: (a) the costs required to get a fully functional case management system in the hands of agents; (b) the extent to which those costs would require additional funding or reprogrammed funds; and (c) what other programs would lose funds, if reprogramming was required. Please provide these assessments to the subcommittee immediately upon completion, or apprise us if they will be delayed beyond 8 weeks.

Answer. The estimate referred to in this question will be based on the IGCEs discussed in response to question 9(C), above. The FBI will keep the subcommittee informed.

Question. In your testimony, you described the FBI's development of an Investigative Data Warehouse (IDW). Was any part of the development of IDW funded out of the $581 million appropriated for the Trilogy project?

Answer. Funds appropriated for Trilogy were not used for the development of the Investigative Data Warehouse.

TERRORIST SCREENING CENTER

Question. In December 2003, the FBI's Terrorist Screening Center began its task of consolidating government terrorist watchlists. In the recent White House budget submission to Congress, an additional $75 million is directed to the Terrorist Screening Center. What is the status of the watchlist consolidation project, and what problems have prevented its completion?

Answer. As of March 12, 2004, the Terrorist Screening Center (TSC) consolidated in the Terrorist Screening Database (TSDB) all identifying data from the 12 watchlists specified in the April 2003 GAO report entitled "Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing" (GAO–03–322). While this consolidated database does include the identifying data from the Automated Biometric Identification System (ABIS) and the Integrated Automated Fingerprint Identification System (IAFIS), it does not include the associated purely biometric information from ABIS and IAFIS.

Question. When will the government have a complete, integrated terrorist watchlist with online access for law enforcement?

Answer. As noted above, the TSC has a complete integrated terrorist watchlist that is now maintained in the TSDB. In addition, information appropriate to pertinent law enforcement groups is exported daily to various information systems, where it is electronically accessible to groups that need it in performance of their specific duties. Domestically, general law enforcement officers have access to the TSDB through the National Crime Information Center system; Customs and Border Patrol and Immigration and Customs Enforcement have access through the Interagency Border Inspection System; the Transportation Security Administration has

access through the No-Fly and Selectee lists; and the Department of State has access through the Consular Lookout and Support System. Among the United States' foreign partners, Australian authorities have access through TACTICS, and Canadian authorities have access through TUSCAN.

CONCLUSION OF HEARING

Senator GREGG. I am going to recess the hearing.

[Whereupon, at 3:20 p.m., Thursday, February 3, the hearing was concluded, and the subcommittee was recessed, to reconvene subject to the call of the Chair.]

○