A Review of the FBI's Trilogy Information Technology Modernization Program

James C. McGroddy and Herbert S. Lin, Editors, Committee on the FBI's Trilogy Information Technology Modernization Program, National Research Council

ISBN: 0-309-09224-8, 78 pages, 8 1/2 x 11, (2004)

A Review of the FBI's Trilogy Information Technology Modernization Program

James C. McGroddy and Herbert S. Lin, Editors

Committee on the FBI's Trilogy Information Technology Modernization Program

Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS **500 Fifth Street, N.W.** **Washington, DC 20001**

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by the Federal Bureau of Investigation (FBI) at its request under Award Number A3D0316801. However, in accordance with NRC policy, the FBI did not review this report before publication, and the opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the FBI.

International Standard Book Number 0-309-09224-8 (Book)
International Standard Book Number 0-309-53248-5 (PDF)

This report is available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu

Printed in the United States of America

Suggested citation: National Research Council, *A Review of the FBI's Trilogy Information Technology Modernization Program*, Computer Science and Telecommunications Board, National Academies Press, Washington, D.C., 2004.

COMMITTEE ON THE FBI'S TRILOGY INFORMATION TECHNOLOGY MODERNIZATION PROGRAM

JAMES C. McGRODDY, IBM (retired), *Chair*
EDWARD BALKOVICH, RAND
RICHARD BASEIL, Holmdel, New Jersey
MATT BLAZE, University of Pennsylvania
W. EARL BOEBERT, Sandia National Laboratories
MARC DONNER, Morgan Stanley
MICHAEL McGILL, Columbus, Ohio
JAMES NOGA, Massachusetts General Hospital
CARL O'BERRY, The Boeing Company
KEN ORR, The Ken Orr Institute
JAMES PATTON, The MITRE Corporation
MARK SEIDEN, MSB Associates
GEORGE SPIX, Microsoft Corporation
CHARLES E. STUART, Competitive Enterprise Solutions, LLC
GIO WIEDERHOLD, Stanford University

HERBERT S. LIN, Senior Scientist and Study Director
KRISTEN BATCH, Research Associate
DAVID DRAKE, Senior Project Assistant (until November 2003)

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

For more information on CSTB, see its Web site at <http://www.cstb.org>, write to CSTB, National Research Council, 500 Fifth Street, N.W., Washington, DC 20001, call at (202) 334-2605, or e-mail at cstb@nas.edu.

Preface

In September 2002, the Federal Bureau of Investigation (FBI) requested the assistance of the National Research Council (NRC) in providing expertise to assist it in its review of the Trilogy information technology (IT) modernization program. In response, the NRC convened a number of experts who met with the FBI. The FBI briefed these experts on various aspects of the program, and these experts responded to the FBI as individuals to those briefings. (In hindsight, many of these individually provided comments presaged the more formal findings and conclusions presented in this report.)

In July 2003, the FBI again requested the assistance of the NRC on the same topic, after having made progress in its IT modernization efforts. The committee's charge was to provide a more thorough review and set of recommendations on the FBI's information technology modernization efforts, focusing primarily on the Trilogy program but addressing related issues as necessary.

In this second request, the FBI asked for a written report, thus invoking the regular NRC report process. To minimize the time needed to respond to the FBI, the Computer Science and Telecommunications Board (CSTB) of the NRC selected a committee composed largely but not exclusively of the experts convened for the September 2002 meeting.

The committee's charge was to review the FBI's efforts on the Trilogy IT modernization program, based on input provided to the committee by the FBI. The FBI also requested a review that could be done quickly and relatively inexpensively. Accordingly, the committee did not systematically develop information from non-FBI sources, nor did it undertake a comprehensive review of all FBI IT systems or plans for such systems. Furthermore, the committee was only able to sample the programs of interest, and thus it did not achieve a comprehensive picture even of those programs. Except as explicitly noted otherwise, the briefings to the committee on October 27-28, 2003, and December 15-16, 2003, constitute the factual base for this effort. The committee's conclusions and recommendations reflect its collective experience with large-scale IT system deployments.

The committee wishes to thank Herbert Lin, the CSTB study director, for his efforts in developing coherent drafts from assorted e-mails and brief notes from committee meetings, and for being the prime driver of the early completion of this report. We also thank the CSTB staff, particularly Kristen Batch for research support, and D.C. Drake for administrative support.

James C. McGroddy, *Chair*
Committee on the FBI's Trilogy Information
Technology Modernization Program

Acknowledgment of Reviewers

This report was reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's (NRC's) Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their participation in the review of this report:

Steven Bellovin, AT&T Research
Ed Feigenbaum, Stanford University
Stuart Feldman, IBM
Robert Grossman, Open Data Partners, LLC
Beryl Howell, Stroz Friedberg, LLC
Sidney Karin, University of California, San Diego
Kenneth Laudon, New York University
Michael Miravalle, Dolphin Technology, Inc.
Joseph Smialowski, Fleet Bank
Robert Spinrad, Palo Alto, California
Howard Wactlar, Carnegie Mellon University
Patrick Webb, Consultant
Todd White, Emerio, Inc.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations nor did they see the final draft of the report before its release. The review of this report was overseen by

Gerry Dinneen (Lexington, Massachusetts). Appointed by the NRC, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

Executive Summary

THE MAIN MESSAGE

Although the Federal Bureau of Investigation (FBI) has made significant progress in its information technology (IT) modernization program in the last year or so, the committee believes that the FBI's IT modernization program is not currently on a path to success. To get on that path, the committee recommends several key changes.

First, foremost, and most critical in light of the impending rollout of the Virtual Case File (VCF) application, the FBI should not proceed with deployment of the VCF until it has a validated contingency plan for reverting completely or partially to the Automated Case Support (ACS) system, if necessary, together with clear and measurable criteria to determine when the ACS can safely be turned off. In the absence of a validated contingency plan, the FBI runs a very high risk that its planned "flash cutover" from the old ACS system to the VCF will cause mission-disruptive failures and further delays. This issue is a consequence of the fact that the VCF has been developed without the benefit of prototyping, with the result that the VCF application will not have been tested in an operational context.

Second, the success of the FBI's information technology efforts will require the development of a close linkage between IT and a coherent view of the bureau's mission and operational needs. The development of this strategic linkage—the enterprise architecture—cannot be delegated inside the bureau to the chief information officer (CIO) or outside to contractors. Only the senior leadership of the FBI can establish the policies, define the operational frameworks and priorities, and make the tradeoffs that are necessary to formulate this strategic view. To do so, they must be deeply and directly involved in its creation.

Third, because testing is such a critical dimension of system development and deployment, the FBI must allow adequate time for testing before any IT application (including the VCF) is deployed, even if dates of initial operational capability are delayed. Testing must include a full systems integration test and adequate scale, volume, and stress tests.

Fourth, the FBI's contract management process is inadequate, and contract schedules lack the specificity necessary to determine whether a project is making adequate progress within schedule and budget constraints. This weakness can be remedied through the aggressive use of standard contract and project management tools.

Finally, while the FBI's IT team includes a number of very capable individuals, the overall human resource base for IT is not nearly adequate to meet the challenges it faces. For Trilogy and subsequent IT projects to have access to the human talent they need to succeed, the FBI must dramatically grow its own internal expertise in IT and IT contract management as quickly as possible.

BACKGROUND

The FBI's Trilogy IT modernization program is intended to upgrade the IT infrastructure of the FBI by providing a high-speed network linking the offices of the FBI, modern workstations and software within each office for every FBI employee, and a user application known as the Virtual Case File to enhance the ability of agents to organize, access, and analyze information. However, the Trilogy program's development and implementation have been troubled. The Trilogy program has been the subject of a number of General Accounting Office (GAO) and Department of Justice (DOJ) inspector general investigations, as well as a source of considerable concern to the U.S. Congress. In July 2003, the FBI requested the assistance of the National Research Council (NRC) to review the Trilogy program and the progress that had been made, and further to consider other nascent IT efforts to support the bureau's new priorities in counterterrorism.

In response to this request, the NRC convened the Committee on the FBI's Trilogy Information Technology Modernization Program, consisting of experts with considerable experience in large-scale IT deployments. The committee met twice in 2-day sessions to receive briefings from the FBI about Trilogy and other related matters, and except as explicitly noted otherwise, those briefings constitute the factual base for this effort.

THE SITUATION TODAY

In the wake of the events of September 11, 2001, the FBI is undergoing a significant expansion of its mission responsibilities and a reordering of its priorities to emphasize its counterterrorist mission, though it still retains its very important criminal investigation mission. The FBI recognizes very well that it will become ever more dependent on information technology in the future to manage the large quantities of information associated with these missions.

It is challenging for any organization engaged in a complex set of activities to introduce new technologies and to reengineer its key processes to exploit them effectively. It is doubly challenging, as it is for the FBI, to do so when under intense operational pressures—the FBI's traditional work must continue while new technology is introduced and while a culture more adapted to the use of IT is evolved. And it is triply so for the FBI in the face of the added strain of its new focus—preventive counterterrorism—in which mission success demands a different mind-set, different operational skills, and the exploitation of an expanded set of information sources.

The FBI has made significant progress in certain areas of its IT modernization program in the last year or so. For example, it has achieved the modernization of the computing hardware and baseline software on the desktops of agents and other personnel, and has taken major strides forward in the deployment of its networking infrastructure. Nevertheless, as this report documents, the committee believes that the FBI's IT modernization program is *not* currently on a path to success. The committee's review of the approach and methodology being used by the FBI has identified significant issues in four major areas: enterprise architecture, system design, program and contract management, and human resources.

ISSUES

Enterprise Architecture

As in any organization, private sector or government, the operational needs of the FBI must be the driver of its information technology investments. If it is to be successful in its efforts to exploit IT, the FBI must *first and as a matter of its highest priority* in its IT efforts formulate an enterprise architecture. Such an architecture is necessary to provide a strategic view of its mission and operational needs, and would begin with a detailed characterization of the bureau's goals, tasks, strategies, and key operational processes. This view links operational objectives and processes to IT strategy and will allow the FBI to specify how investment is tied to the achievement of operational objectives.

Based on presentations to the committee by the FBI (as well as a review of certain documents produced by the FBI, GAO, and DOJ), the committee has concluded that the FBI's efforts and results in the area of enterprise architecture are late and limited, and fall far short of what is required. The committee was encouraged by early efforts driven by the recently appointed executive assistant director of intelligence to develop a concept of operations of the intelligence process from which appropriate IT systems support can be architected and designed. However and overall, the FBI's senior leadership is insufficiently engaged in the development of the enterprise architecture, with the result that this development task is delegated in large part to outside contractors and to a CIO. Though these parties are essential players, only the senior leadership of the FBI can establish the key policies, set the operational priorities, and make the significant tradeoffs that must be reflected in the complete enterprise architecture and IT system design. Among the most important decisions to be made are the risk tradeoffs involved in ensuring sufficiently broad controlled access to sensitive information. Such decisions must be made at the level of the senior leadership.

System Design

Although the committee recognizes that the bureau has made significant progress on the Virtual Case File in the last year or so, it has concerns about the VCF and the Integrated Data Warehouse.

The VCF has many positive attributes. Based on a canned demonstration of a VCF mock-up, the committee believes that the VCF should significantly enhance the information management capabilities of FBI agents in their investigative role. However, the bureau-wide rollout of this application is months delayed from its originally scheduled deployment in December 2003. Going forward, the committee has a number of concerns about the VCF.

First, the FBI described to the committee a plan for a "flash cutover" from the old Automated Case Support system to the VCF, rather than a limited initial rollout that would shake out problems in an operational context. The committee's concerns in this area are heightened by the fact that in the interests of rapid deployment, the current VCF schedule appears to give little consideration to testing and presumes success at every stage—a highly risky approach. The current choice facing the FBI on this matter of scheduling is between (a) delaying VCF deployment so that adequate testing can be completed, and (b) forcing operational users to do the testing themselves after implementation, with all of the potential negative consequences that such an approach can produce. The current plan is likely to result in (b).

With limited testing, and no experience gained from a limited initial rollout, the FBI would be implementing what amounts to a prototype throughout the bureau. This approach is nearly guaranteed to cause mission-critical failures and further delays, with implications for training, performance, coherence, internal morale, public image, and cost to recovery.

Second, the VCF was designed to support the investigative mandate of the FBI. The design process was well under way prior to the expansion of the intelligence mission, and the requirements for the processes supporting the intelligence mission were not included in the VCF design. For this reason, and because of the significant differences in IT requirements between systems supporting investigation and those supporting intelligence, the committee strongly recommends that the FBI refrain from using the VCF as the foundation on which to build its analytical and data management capabilities for the intelligence processes supporting the counterterrorism mission. Rather, the FBI should conceptualize an architecture for the counterterrorism mission from scratch, and then design explicit interfaces to the VCF when information must flow between them.

Another application, still in the design stage, the Integrated Data Warehouse (IDW), also seems to suffer from a lack of deep consideration of how and what sources of data are used by different operational elements and in different processes of the FBI. For example, presentations to the committee suggested a mismatch between the expectation that intelligence analysts would have access to live databases containing the most current information and the reality of what the IDW as designed would actually provide. That is, the IDW would provide only the latest copies of production databases, replacing old copies of data with newer copies. Thus, data could be there one day and not the next, since the IDW apparently was not designed to retain older or historical data. While having only the most recent copy of data may be appropriate for the purposes of an investigation (presuming the most recent copy is the most accurate and reliable), this process may not serve intelligence purposes very well.

Program and Contract Management

The committee has serious concerns about the approaches and processes used by the FBI to develop and field both IT infrastructure and applications.

In the committee's view, a major weakness is that the FBI does not appear to employ user-vetted prototypes in its applications development process. In practice, it 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. Therefore, internal development plans, and the development contracts with supporting organizations, should call for an approach that is based on a process of extensive prototyping and usability testing with real users. Doing so allows iterative development with strong user feedback and involvement, thus increasing the chances that what is ultimately delivered to the end users meets their needs. This point is relevant to many dimensions of system development, including the functionality desired in a new application, the convenience and intuitiveness of a user interface, and the nature, scale, and mix of the data entry, management, and retrieval load that the networks and systems must support under real operational conditions.

The committee believes that both contract management and program management need substantial improvement. For example, while task orders viewed by the committee detailed pricing to eight or nine significant figures, the corresponding contract schedules were almost totally lacking in specifications, deliverables, and commitment to checkpoints. Under these circumstances, effective program and contract management is essentially impossible. Current contracting and management problems, aggravated by frequent turnover among key FBI staff, make it unsurprising that Trilogy is significantly behind schedule and over budget.

Furthermore, the FBI appears overly dependent on outside contractors to undertake essential tasks, such as identifying key operational processes, defining the FBI's IT concept of operations, and making decisions about the major tradeoffs that are inevitably required. While outside contractors play important roles, it is the senior FBI management who must lead in assuming responsibility for these tasks.

Human Resources and External Constraints

Although the committee did not undertake a comprehensive assessment in the human resources area, presentations to the committee persuaded it that with a few exceptions, the FBI lacks a human resource and skill base adequate to deal with the bureau's IT modernization program. Specifically, the FBI is extremely short on experienced program managers and contract managers and senior IT management team members with good communications skills. At the same time, the FBI appears to have the authority to hire highly qualified IT personnel without requiring them to make excessive financial sacrifices, and to borrow personnel from other agencies and even from the private sector. The committee is encouraged to learn that an acting chief information officer was put into place at the beginning of 2004.

Of lesser concern, but in the committee's view still worth noting, is the fact that the FBI also operates under a number of external constraints that diminish its management flexibility. For example, it is the committee's understanding that the FBI is unable to take actions such as reprogramming amounts in excess of $500,000 without explicit congressional approval. This constraint is inconsistent with the expectation that the FBI will move quickly and forcefully to reshape itself to deal effectively with new challenges.

RECOMMENDATIONS

The first and most urgent recommendation, indeed critical in light of the impending VCF system rollout, is that the FBI not proceed with deployment of the VCF until it has a validated contingency plan for reverting completely or partially to the ACS, if necessary, and clear and measurable criteria to determine when the ACS can safely be turned off. Beyond this critical recommendation, the committee makes a number of recommendations, grouped into four areas, that will significantly increase the likelihood of success in and drive an accelerated pace for the FBI's IT modernization efforts. The most important of these recommendations are described below, and they are, in the committee's judgment, imperatives for the success of the FBI's IT modernization program.

In the area of enterprise architecture, the development of a complete enterprise architecture is central to the FBI's IT efforts. The most important recommendations in this area (others are presented in the main text) are the following:

- If the FBI's IT modernization program is to succeed, the FBI's top leadership, including the director, must make the creation and communication of a complete enterprise architecture a top priority. This means that they must be personally involved and invested in the key decisions that the process will require be made, such as the tradeoffs between the security of and access to information in the various data sources that are used in criminal investigation and counterterrorism efforts. While a contractor might well assist the FBI in developing the enterprise architecture, no contractor will fully understand the operational issues that must be reflected in the enterprise architecture, nor be empowered to make decisions about how to make the tradeoffs with competing concerns. A small team, consisting primarily of senior operational managers from the Criminal Investigation Division, the Office of Intelligence, and the Counterterrorism Division, and a senior IT executive to translate what these managers say into architectural terms, should be able to develop the broad outlines of the operational aspects of the enterprise architecture as well as a top-level schematic view of the systems design in a matter of 4 to 6 months of full-time work. To decide on the many operational and policy tradeoffs that will inevitably arise, this team must have direct access to and the frequent involvement of the most senior management of the FBI, including the director and the deputy director.
- The FBI should seek independent and regular review of its enterprise architecture as it develops by an external panel of experts with experience in both operations and technology/architecture. When the first draft of the enterprise architecture has been prepared, it should be reviewed by an external panel of independent experts charged with helping the FBI to improve how it uses IT in the long term.
- Given that the counterterrorism mission requires extensive information sharing, the FBI should seek input on and comment from other intelligence agencies regarding its enterprise architecture effort. The reason is that the FBI's information systems must have interfaces to those agencies to ensure that the information resources of those agencies are appropriately linked to FBI systems so that those agencies are able to work collaboratively.

In the area of system design, the most important recommendations (others are presented in the main text) are the following:

- The FBI should refrain from initiating, developing, or deploying any IT application other than the VCF until a complete enterprise architecture is in place.
- The FBI should develop a process map for information sharing that clearly defines the current state of and a desired end state for the information-sharing process so that the numerous information-sharing initiatives can be coordinated and properly monitored and managed.
- The FBI should immediately develop plans that address recovery of data and functionality in the event that essential technology services come under denial-of-service attacks (e.g., from viruses and pervasively replicated software bugs).

In the area of program and contract management, the most important recommendations (others are presented in the main text) are the following:

- Because testing is such a critical dimension of system development and deployment, the FBI must allow adequate time for testing before any IT application (including the VCF) is deployed, even if dates of initial operational capability are delayed. Testing must include a full systems integration test and adequate scale, volume, and stress tests.
- In future IT applications development, particularly of large-scale end-user-oriented applications, procurement contracts should be conditioned on the development of small-scale prototypes that can be built rapidly and tested with user feedback before committing to large-scale development.
- For IT applications beyond the VCF, the FBI should exploit proven methodologies of contracting and contract management, including the use of detailed functional specifications, specific milestones, frequent contract reviews, and earned-value metrics.

In the area of human resources, the most important recommendations (others are presented in the main text) are the following:

- For Trilogy and subsequent IT projects to have access to the human talent they need to succeed, the FBI must dramatically grow its own internal expertise in IT and IT contract management as quickly as possible. In the short term, this effort will almost certainly involve borrowing experienced and capable contract managers from other agencies. In the long run, establishing its own internal IT expertise will involve the creation of long-term high-status career tracks with the FBI for IT personnel.
- Because of their importance to the short- and long-term success of the bureau's IT modernization efforts, the FBI must permanently fill the positions of chief information officer and chief enterprise architect, and the committee concurs with the director's judgment that filling these positions with appropriately qualified individuals ought to have the highest priority.
- The FBI should develop an improved system for internally reviewing the state of progress in key IT programs and for communicating relevant findings to key stakeholders, thus preempting the perceived need for and distraction of constant external investigations.

The committee believes that the FBI has made significant progress in some areas of its IT modernization efforts, such as the modernization of the computing hardware and baseline software and the deployment of its networking infrastructure. However, because the FBI IT infrastructure was so inadequate in the past, there is still an enormous gap between the FBI's current IT capabilities and the capabilities that are urgently needed.

Some useful and valuable returns from the investment in the Trilogy program appear to be within reach. Nevertheless, the committee believes that a major effort is needed to bring the FBI to the state where it can be characterized as an effective exploiter of information technology. The committee has made recommendations that, if adopted, will significantly increase the likelihood that the FBI's Trilogy IT modernization program will enhance the FBI's effectiveness in carrying out its crime-fighting and counterterrorism missions. But it emphasizes the difference between a pro forma adoption of these recommendations and an adoption of these recommendations that is both fully embraced throughout the agency and aggressively executed. The former may be the metric that auditing and oversight agencies and offices often use in assessing agency performance, but it is the attitude and willingness of senior staff to act that really count. The senior management of the FBI has a substantive and direct role to play in the FBI's IT modernization efforts. This role either has not been understood or it has been given a lower priority based on the perception of more immediate operational priorities. Given the importance of IT to the FBI's future success in carrying out its missions, the FBI's senior management must concern itself as much with developing a coherent vision for using IT as with budgets, training programs, equipment, and organization. As the complexities of the FBI's evolving role are understood, the committee believes that investment by the FBI's senior management team in the IT process will yield major enhancements to mission achievement as well as substantial operational efficiencies.

1

Background

The Federal Bureau of Investigation (FBI) is undergoing a significant shift of its mission responsibilities and a reordering of its priorities. For most of its history, the FBI has been oriented primarily toward law enforcement and the investigation of criminal activities. However, in the wake of the attacks of September 11, 2001, the threat environment has changed dramatically, and the FBI's mission has expanded to include as its top priority the detection of potential terrorism against the U.S. homeland and the interdiction of terrorist activities before they cause damage. Although the leadership of the FBI recognizes the need for upgraded information technology (IT) to enhance its ability to collect, store, search, retrieve, analyze, and share information in pursuit of its missions, the FBI has not been regarded as a sophisticated user of IT. Indeed, for many years, the FBI has been criticized for inadequate attention and competence with respect to its use of IT.

For any organization engaged in a complex set of activities, the introduction of modern IT and the concomitant reengineering of the organization's key processes to fully exploit the technology constitute a major challenge. In the FBI's case, this transformation is being managed under intense operational pressures: the FBI's traditional work must continue even as new technology is introduced and a culture more comfortable with IT is evolved. Compounding this challenge is the added strain of the new focus on preventive counterterrorism, where success demands a different mind-set, different operational skills, and the exploitation of a radically expanded set of information sources.

The FBI has made significant progress in certain areas of its IT modernization program in the last year or so. For example, it has achieved the modernization of the computing hardware and baseline software on the desktops of agents and other personnel and has taken major strides forward in the deployment of its networking infrastructure. Nevertheless, in a number of key areas, the FBI's progress has fallen significantly short of what it, and the nation, require.

Organizations should invest in IT only if such investment will improve their operational effectiveness. Therefore, the return on an IT investment must be measured in operational terms—more and better results, increased responsiveness and agility, and improved efficiency of operations. Maximizing the return on a major IT investment thus requires an intimate and dynamic interplay between the technology and an organization's operational strategy, and so this report begins its discussion from the operational and strategy side.

1.1 PRELIMINARIES

Information technology most effectively facilitates the "business" and "operations" of organizations when it is explicitly designed to do so, whether the organizations are profit-and-loss enterprises, not-for-profit private organizations, or government agencies. Such design requires careful specification of objectives, strategies for achieving objectives, and the processes by which strategies are realized. Effective management also requires that a set of measures of success be defined and tracked, using both outcome and process metrics. This report makes frequent use of the term "operational processes" to refer to the processes used within the FBI to accomplish its missions. (Some might prefer the term "business processes"; the meaning is the same.)

The committee views the FBI as being engaged in a number of important operational pursuits that are tantamount to enterprise business objectives, even though those operational pursuits do not have profit-making goals. Thus, the FBI should engage in cost-effectiveness analyses corresponding to cost-benefit analyses in commercial enterprises that will aim to increase the return in improved operational effectiveness and efficiency that U.S. taxpayers rightly expect for bureau expenditures.

In general, organizations must develop their own metrics to quantify their objectives. Among the purposes of doing so are to be able to determine the extent to which a given investment will help an organization better achieve those objectives, and to retrospectively track the returns on such investments. The committee recognizes that the ultimate goal of the FBI is the *prevention* of undesirable events, and in this context, meaningful quantification of that goal can be problematic. Nevertheless, it is desirable and almost always possible to establish reasonable intermediate quantifiable objectives that bear on operational efficiency, subject to the understanding that these measures reflect the underlying processes and do not become goals in and of themselves.

The committee believes that many management approaches, tools, and best practices from the commercial sector are applicable to the FBI, just as they are to the Department of Defense and other government enterprises. Many of the observations and recommendations in this report are the result of the committee's assessment of the FBI's current approach compared with successful approaches seen by committee members in both the for-profit and the not-for-profit sectors.

1.2 MISSIONS OF THE FBI

The nature of an organization's missions and its strategy and operational objectives are the primary drivers of the kinds of information and communication it needs and the processes it must exploit. These needs in turn determine the architecture, design, and functioning of its IT systems.

According to the FBI, its mission is "to uphold the law through the investigation of violations of federal criminal law; to protect the United States from foreign intelligence and terrorist activities; to provide leadership and law enforcement assistance to federal, state, local, and international agencies; and to perform these responsibilities in a manner that is responsive to the needs of the public and is faithful to the Constitution of the United States."[1] The first two elements are highly operational: the investigation of criminal activity to support the prosecution of criminals ("criminal investigation" for short in this report) and the prevention of terrorism within the United States and against U.S. interests around the world ("counterterrorism" in this report). Supporting these missions and the achievement of the related operational objectives of these mission segments is a set of key processes that are used to different degrees in achieving the objectives.

1.2.1 Criminal Investigation

The traditional mission of the FBI is that of an investigative agency for the Department of Justice of the United States. This mission is focused on investigating and preparing much of the information basis for the prosecution of crimes. The information developed by FBI investigators is provided to prosecutors who in turn determine if an individual will be prosecuted. The FBI can initiate a criminal investigation when facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed, and the investigation may be conducted to prevent, solve, and prosecute such criminal activity.[2] As a practical matter, most investigations are *reactive*—that is, they are initiated in response to a specific occurrence of criminal activity. (Note that the standard for "reasonable indication" is substantially lower than that for probable cause.) Once the FBI investigative activity has been initiated, the FBI will use the resources legally at its disposal to gather relevant information related to the situation.

In those instances where a criminal act may be committed in the future, preparation for that act can be a current criminal violation under the conspiracy or attempt provisions of federal criminal law or other provisions defining preparatory crimes, such as solicitation of a crime of violence or provision of material support in preparation for a terrorist crime. The standard for opening an investigation is satisfied where there is not yet a current substantive or preparatory crime, but facts or circumstances reasonably indicate that such a crime will occur in the future.[3]

1.2.2 Counterterrorism

In the counterterrorism domain, the FBI's objective is to prevent acts of terrorism in the United States and against U.S. persons and interests throughout the world. Accomplishing this daunting objective requires, among many other activities, accessing, analyzing, and

[1] See http://www.fbi.gov/priorities/priorities.htm.

[2] A step short of a full-fledged investigation is known as a preliminary inquiry, which is a step taken when the FBI receives information or an allegation not warranting a full investigation—because there is not yet a "reasonable indication" of criminal activities—but whose responsible handling requires some further scrutiny beyond the prompt and limited checking out of initial leads. Such an inquiry is intended to allow the government to respond in a measured way to ambiguous or incomplete information, with as little intrusion as the needs of the situation permit. This measured response is especially important when an allegation or information is received from a source of unknown reliability. A preliminary inquiry is intended to establish whether or not a full-fledged investigation is warranted.

[3] Information on investigations and inquiries is derived from *The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations*, available at http:// www.usdoj.gov/olp/generalcrimes2.pdf.

exchanging massive amounts of information, and close, daily coordination and cooperation among law enforcement, intelligence, and many other involved organizations.[4]

In this area, the role of the FBI is *proactive* and ongoing, and the execution of its mission is not necessarily carried out in response to any particular external event. (If a serious terrorist event has already occurred, then it is reasonable to suggest that the execution of the counterterrorism mission has not been fully successful.) There is some overlap of activities between the criminal investigation and counterterrorism missions, as discussed below, but the new emphasis on counterterrorism requires a different mind-set among some FBI staff, some new or different operational processes, and new requirements for supporting IT systems.

1.3 KEY FBI PROCESSES

It is important to distinguish between missions and the key processes that support the accomplishment of those missions. In some cases, a key process supports only one mission; in others, a key process may support more than one mission. The key processes used by the FBI involve, among other things, information acquisition and the workflow of information management—how information is acquired, who must act on it, how information of all types flows within the organization, how it must be processed and analyzed, and what types of inferences must be drawn. For information-intensive missions such as criminal investigation and counterterrorism, modern IT and its proper design and exploitation are critical contributors to truly effective processes.

This section describes some of the key processes within the FBI. However, the reader should keep in mind that the terminology used here reflects processes rather than organizational titles. That is, "investigation," "intelligence," and "information management" are meant to refer to processes or functions rather than specific offices or divisions within the FBI.

1.3.1 Investigation

The investigative process is the primary process supporting the law enforcement mission. Investigation develops information from a variety of sources, including but not limited to information gathered directly by special agents or other law enforcement agencies, information obtained through informants, information obtained from other agencies such as Customs and Border Protection or local or foreign law enforcement agencies, laboratory-developed information, and publicly available information (e.g., information on the Internet or in the news). The collection and analysis of information are usually under the control of a special agent leading and directly responsible for the investigation. The information (or derivatives, such as pointers to certain collected information) is placed in centralized FBI files for appropriate dissemination and use as part of the case file.

The agent or group of agents assigned to a case is the focal point of FBI criminal and law enforcement activities. The agent is responsible for carrying out the investigative task and

[4] Another dimension of the counterterrorism mission is the active insertion of sympathetic parties (ranging from those who listen to those who take a more active role in disrupting) into hostile organizations such as terrorist cells. This type of activity is far more controversial as it poses nontrivial challenges to the nation's core values, and history demonstrates that such actions can have significant political repercussions when they are undertaken within the United States. In any event, this report is deliberately silent on this dimension of the counterterrorism mission, as it is largely beyond the scope of the committee's charge.

managing much of the information involved. In the case of a criminal investigation, the information developed is then conveyed to the prosecutor for decision and action. In the case of a background investigation, the information is delivered to the requesting agency. The agent is the focal point of the activity with support from administrative staff, analysts, and other FBI employees. The investigative information is organized around cases, which serve as the fundamental unit for information management. Moreover, there are a variety of legal and procedural requirements in place to ensure that developed information can be used in court to support prosecutorial activities.

The FBI relies extensively on a well-developed remote tasking practice whereby an agent in one location who needs information from another area can easily transmit a request, called a "lead," to the appropriate field office where it will be followed up by a local agent. This practice is remarkable in that it allows the organization to function on a continental scale without a tremendous cost in time and money for travel or the overhead that would be involved if headquarters had to be directly involved. Yet the process provides the personal contact that is essential to productive interviewing by FBI agents of suspects or individuals with leads. For this practice to work as effectively as it manifestly does is a testimony to the quality of training and the uniformity of culture within the FBI. Nevertheless, a thoughtful application of technology can support and enrich this practice, and make it even more effective and efficient.

1.3.2 Intelligence

Intelligence processes include information collection and analytical functions. Information gathered under intelligence auspices is frequently more tentative and expansive in scope as compared with information collected under investigative auspices. Rules on information retention and use also differ in each domain. Intelligence processes are used in both law enforcement and counterterrorism missions, although the collection of information gathered under intelligence auspices is not directly aimed at the support of prosecutorial activities.

Intelligence in the counterterrorism context requires that voluminous information resources from internal and external sources be logically brought together and analyzed with the goal of identifying potential threats of, or precursors to, terrorist activity. The range of sources of information that must be selectively probed and analyzed is enormous, and much of the information will be obtained not from government-owned sources but from publicly available sources, such as newspapers in foreign languages, or the Internet.[5]

[5] To illustrate one problem, the name of an individual can be represented in multiple ways. A specific name can have different variants (e.g., with or without a middle name, nicknames, short forms, order of given and family names). An individual may be regularly identified with different name variants in different geographical locales (even within the same country). Transliterations into Western languages (e.g., of Arabic, Chinese, or Cyrillic into Roman alphabets) add another layer of complexity. Names transcribed from voice (e.g., a wiretap) may be highly ambiguous in spelling. The original material from which the name was obtained (fax, Web, e-mail, and so on) may be rendered in a multitude of computer encodings. Search engines used for intelligence purposes must be able to reconcile all of these different encodings of a name when an analyst is searching on a given name for references to a given individual. When the committee asked the FBI about this issue during briefings, the reply received was, "We intend to use Unicode to represent names." Unicode representations deal with part of the problem (the part dealing with the ability to represent a name in its native alphabet), but not the other parts of the problem. Note that these issues also arise in criminal investigations, but to the extent that investigations relate to crimes committed by people in the United States, issues related to names rendered in non-native alphabets arise with much lower frequency.

Analytical functions in the intelligence process must analyze information of uncertain relevance and quality. The desired result is the distillation of conclusions that become increasingly certain as they are further aggregated and refined. Such analyses may, at different stages, result in warnings and may initiate deeper and more focused investigations that may eventually lead to prosecutions.

The intelligence process generally requires that the FBI receive information from and disseminate information to local law enforcement agencies, the U.S. intelligence community, and often agencies of foreign nations. The ability to share information at multiple levels of security classification with a wide variety of collaborators is essential to the underlying intelligence process and to performance of the counterterrorism mission. Information sharing must generally proceed with much more caution in counterterrorism efforts than in most criminal investigations because of the sensitivity of information sources. Yet strong capabilities to access, manage, analyze, and communicate information across institutional boundaries are key to the analytical function at the core of the intelligence process.

Sharing information requires cooperative relationships with the intelligence and law enforcement communities across jurisdictional levels from local to international. Furthermore, its success demands a framework of policy and process to ensure appropriate balance among timely access, security, and privacy rights. Trained analysts probe, tease apart, and develop new information that can identify, confirm, or exclude a hypothesis or a threat. IT should serve to facilitate mutually cooperative relationships and analytical activities.

In the law enforcement mission, special agents are in the lead, and analysts supporting those agents must understand the investigative role of the bureau and the agent's operational processes. In the counterterrorism mission, analysts are primary, and the agents supporting those analysts must understand that the primary role of analysts in counterterrorism is analogous to the role that agents play in pursuing the law enforcement mission. (For example, according to the FBI's Office of Intelligence, special agents constitute one of the best collection mechanisms available to the intelligence community for counterterrorism work.)

Most analysts have specialized expertise but must be able to easily cooperate with colleagues on diverse topics. An individual analyst at the FBI must be highly skilled in the methods and processes that are used for both the criminal and the counterterrorism missions. Analysts must be comfortable with the IT that provides the means of access to raw information and underlies tools to support the distillation, sharing, and analysis processes.

1.3.3 Information Management

The investigative and intelligence processes used by the FBI are information-intensive, and the bureau has recognized that state-of-the-art information management that exploits available technology can significantly enhance the effectiveness and efficiency of these processes. Furthermore, both counterterrorism and criminal investigation are evolving in a way that spans traditional organizational boundaries in the FBI. Special agents in charge (SACs) are organized around geography. Terrorism and crime no longer respect those boundaries, and thus a bureau-wide technology deployment necessarily entails a set of systems and data that can be accessed easily across the geographic reach of the FBI's missions. (The FBI encompasses 56 field offices in major cities in the United States, approximately 400 resident agencies (i.e., satellite offices in smaller cities and towns), and foreign posts in 52 nations.)

Driven initially by the need for improved support of the investigative process, the FBI has embarked on a major IT modernization program, whose main focus today is the Trilogy program. Trilogy has two major objectives. The first is the creation of a more modern end-user-oriented infrastructure, consisting of a secure wide-area network and related local area networks, together with modern workstations, printers, scanners, and a base of commercial software applications such as browsers. This infrastructure is intended to provide an enhanced platform for modern applications.[6] The second objective of Trilogy is to provide enhanced support of the investigative process. This objective is the focus of the Virtual Case File (VCF) that will provide via a browser interface a user-friendly capability for agents to electronically manage case-related information critical for criminal investigation.

At this writing (late March 2004), neither the infrastructure deployment nor the VCF application is complete, although significant progress has been made on both. In addition to the original two objectives, a general requirement to support the counterterrorism mission has also been placed on Trilogy, although specifications for that novel task have not been fully developed. The FBI has also embarked on the development and implementation of systems to support its intelligence functions, which are also important to the counterterrorism mission. Central to this thrust is the creation of a large data repository, referred to as the IDW, the Integrated Data Warehouse, also in its early stages.

[6] As used in this report, the term "platform" refers to the computing infrastructure supporting FBI applications, specifically the combination of a type of hardware, say a PC-compatible personal computer, and specific software, such as a specific operating system, Web browser, and set of basic office applications.

2

IT-Related Issues for the FBI Requiring Immediate Action

Although limited in scope and time, the committee's review of the approach and methodology currently being used by the FBI to drive the introduction of its new IT systems has raised a number of significant issues. To address these issues requires concerted FBI action in four major clusters. The issues in each of these clusters are serious in and of themselves. Taken in aggregate, the detrimental impact of inattention to these issues on the FBI's IT modernization efforts is enormous despite the progress that has been made. These four clusters are:

- *Enterprise architecture.* An enterprise architecture maps the linkage between the FBI's strategy and operational needs and its IT program.
- *System design.* System design is the engineering of detailed IT solutions driven by the enterprise architecture.
- *Program and contract management.* Large-scale program and contract management processes are critical to the success of IT modernization endeavors as massive as Trilogy.
- *Skills, resources, and external factors.* The fourth and final cluster cuts across the first three clusters and generally relates to human resources and skills, and to some of the external constraints faced by the FBI in its IT modernization efforts.

The next four sections deal with these issues cluster by cluster.

2.1 ENTERPRISE ARCHITECTURE ISSUES

2.1.1 Creating an Enterprise Architecture That Serves FBI Objectives

What Is an Enterprise Architecture?

An enterprise architecture characterizes the enterprise's missions, tasks, and operational processes, and relates these tasks, processes, and operational objectives to IT strategy, investment, and design. It provides substantial detail on the structure and standards used to implement the IT system. The enterprise architecture is the framework that describes the way in which an organization such as the FBI conducts its mission(s), how it organizes and uses technology to accomplish its goals and execute key operational processes, and how the IT system is structured and designed in detail to achieve these objectives. In general, it should also include documentation that explains the rationale behind important decisions and why certain alternatives were chosen and others rejected.

An enterprise architecture thus contains much more than information about technology. The enterprise architecture becomes the template on which the IT investment is rationalized, and the enhancements to the FBI's mission achievement, the return on the investment, are defined and quantified using appropriate metrics. When new needs emerge, as with the counterterrorism mission, an enterprise architecture provides a point of departure—a framework within which additional capabilities can be coherently designed.

Absent an enterprise architecture, it is essentially impossible for any large organization, including the FBI, to make coherent or consistent operational or technical decisions about IT investments. Among these decisions are the definitions of appropriate data structures and linkages to other systems and data sources, policies and methods of information sharing, issues of security and the tradeoffs with information access, innovation, and the exploitation of evolving technologies, and metrics of effectiveness for the IT system and its use.

The close link between good enterprise architecture planning and sound systems engineering practice on the one hand and success in large-scale IT deployments on the other has been demonstrated in numerous examples in the private sector and in the federal government.[1] Further, the existence of the enterprise architecture can be a major contributor to the confidence and trust that management, users, and implementers have in a project, as well as facilitating cooperation among them. A well-documented and communicated enterprise architecture is a prerequisite for driving cultural and operational change and innovation at a pace that effectively capitalizes on the pace of technology improvement. Good models depict the as-is (today's) environment as well as the to-be (future desired) environment, showing the transition.

The Structure of an Enterprise Architecture

While technology capability is an important input to operational strategy, it is important that IT investment not be driven primarily from the technology end, but rather that operational strategy drive technology investment and system design. To this end, the committee believes that a good starting point for achieving the required linkage is to think about architectures in three conceptually distinct but interrelated forms:[2]

[1] For an example in a medical setting, see Jonathan M. Teich et al., "The Brigham Integrated Computing System (BICS): Advanced Clinical Systems in an Academic Hospital Environment," *International Journal of Medical Informatics* 54: 197–208 (1999). For a case study in which failure was closely associated with insufficient attention to architectural issues, see National Research Council, *Continued Review of the Tax Systems Modernization of the Internal Revenue Service*, Computer Science and Telecommunications Board, National Academy Press, Washington, D.C., 1996. For a case study in the private sector that demonstrates similar lessons, see Christopher Koch, "AT&T Wireless Self-Destructs," *CIO Magazine*, April 15, 2004, available at http://www.cio.com/archive/041504/wireless.html.

[2] The architectural triad used here originates with the Department of Defense, which has used this framework to develop its command and control systems since 1997. (A good reference on this subject is Architecture Working Group, Department of

- *An operational architecture*, which describes in graphical and narrative terms the key operational objectives; the operational elements, tasks, and processes used to achieve them; a high-level description of the types of information used and created; how and with what constraints information of various types must be exchanged; and the information flows in these processes. An operational architecture relates to specific mission scenarios and functions and forms the basis for realistic process and information flow representation and prioritization.[3] (An analogy for operational architecture in the construction domain is the concept of operations for the various purposes a building will serve, and how various components of the building will serve those needs.)
- *A systems architecture*, which describes at a high level the data repositories, systems, applications, connectivity, and communications infrastructure that supports the operational architecture for mission needs. The systems architecture defines the logical and physical connection, location, and identification of the key nodes, circuits, networks, and platforms that are associated with information exchange and specifies some critical system performance parameters. The systems architecture is constructed to satisfy operational architecture requirements using the standards defined in the technical architecture. (An analogy for systems architecture in the construction domain is the blueprints for a building that illustrate how components fit together.)
- *A technical architecture*, which captures the key technical standards, protocols, and specifications required to implement the systems architecture. A technical architecture is intended to be a compact set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conforming system satisfies a specific set of requirements. It identifies system services, interfaces, standards, and their relationships. It provides the framework for the derivation of engineering specifications that guide the implementation of systems. (An analogy for technical architecture in the construction domain is the set of building codes for connecting subsystems and ensuring the operational effectiveness of the building with the community electrical, water, sewage, and roadway systems.)

To indicate what some of the content of these three architectures might be, the committee attempts to describe in Figure 1 some primary and supporting activities in the FBI as they might contribute to one part of the architectural triad described above—an operational architecture.[4] The purpose of Figure 1 is to focus attention on key structural elements of the FBI. Figure 2 shows a subset of FBI activities and the potential scope of planned supporting IT

Defense, *C4ISR Architectural Framework, Version 2.0*, December 18, 1997, available at http://www.defenselink.mil/nii/org/cio/i3/AWG_Digital_Library/pdfdocs/fw.pdf. The descriptions of operational, systems, and technical architectures contained in this report are adapted from this DOD document.) Note, however, that the engineering methodology of defining a "functional architecture" based on processes and information flows and then building a "system architecture" with ever increasing technical detail dates back to the mid-1970s. And the use of structured analysis to form the basis for a technical system design has been in widespread use throughout commercial and government organizations since the late 1970s.

[3] As one possible scenario, the FBI told the committee that it has some 6 million documents found in Afghanistan. How will the information in these documents be extracted and managed? Who will have access to what set of those documents? What circumstances will govern access rules? How will the information contained in these documents be used with other information to which the FBI has access? Thinking through this scenario will provide a great deal of insight into information management requirements. The key point is that however the FBI decides to handle the information from these documents, it should be able to articulate the rationale for doing so in terms that make sense from an operational point of view.

[4] See, for example, Michael E. Porter, *Competitive Advantage: Creating and Sustaining Superior Performance*, Free Press, New York, 1998.

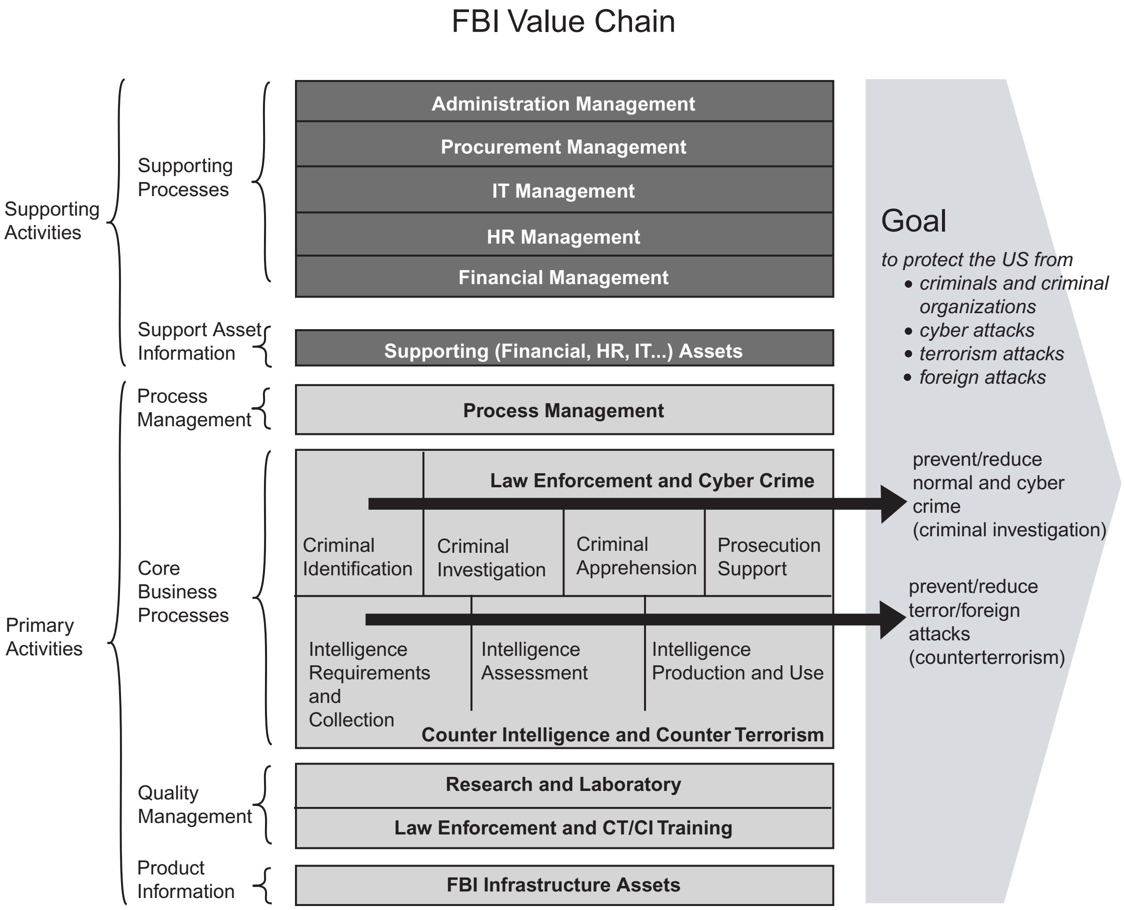
FBI Value Chain
Supporting Activities
Supporting Processes
Administration Management
Procurement Management
IT Management
HR Management
Financial Management
Support Asset Information
Supporting (Financial, HR, IT...) Assets
Primary Activities
Process Management
Process Management
Core Business Processes
Law Enforcement and Cyber Crime
Criminal Identification
Criminal Investigation
Criminal Apprehension
Prosecution Support
Intelligence Requirements and Collection
Intelligence Assessment
Intelligence Production and Use
Counter Intelligence and Counter Terrorism
Quality Management
Research and Laboratory
Law Enforcement and CT/CI Training
Product Information
FBI Infrastructure Assets
Goal
to protect the US from
• criminals and criminal organizations
• cyber attacks
• terrorism attacks
• foreign attacks
prevent/reduce normal and cyber crime (criminal investigation)
prevent/reduce terror/foreign attacks (counterterrorism)

FIGURE 1 FBI value chain—an example of a framework for "the view from 40,000 feet" of a serious enterprise architecture. This adaptation of Michael Porter's famous business value chain indicates the core processes of the FBI's two major missions—(1) criminal investigation and (2) counterterrorism. In addition, the primary activities include process management to monitor the performance of these two missions and quality management to provide feedback on the effectiveness of both the primary outputs—information—and how users actually use that information. At the top of the diagram are the traditional resources management areas: administration, procurement, human resources, finance, and IT. These supporting activities ultimately must be integrated with the primary activities shown in the bottom two-thirds of the diagram for the FBI to work most effectively.

activities—the ACS, the VCF, SCOPE (the Secure Counterterrorism Operational Prototype Environment, discussed below in Section 2.2.3), and the IDW.

Figures 1 and 2 represent the committee's (certainly imperfect) perspective on FBI operations and the roles of IT systems in supporting FBI missions. These figures are highly simplified (for example, they do not include the operational impact of providing law enforcement assistance to other agencies), and they lack any kind of supporting detail. However, the committee *inferred* the content of Figures 1 and 2, rather than receiving them from the FBI. One of the committee's major concerns is that it was not shown anything produced by the FBI or its contractors that approaches the content or substance of even these oversimplified figures. In

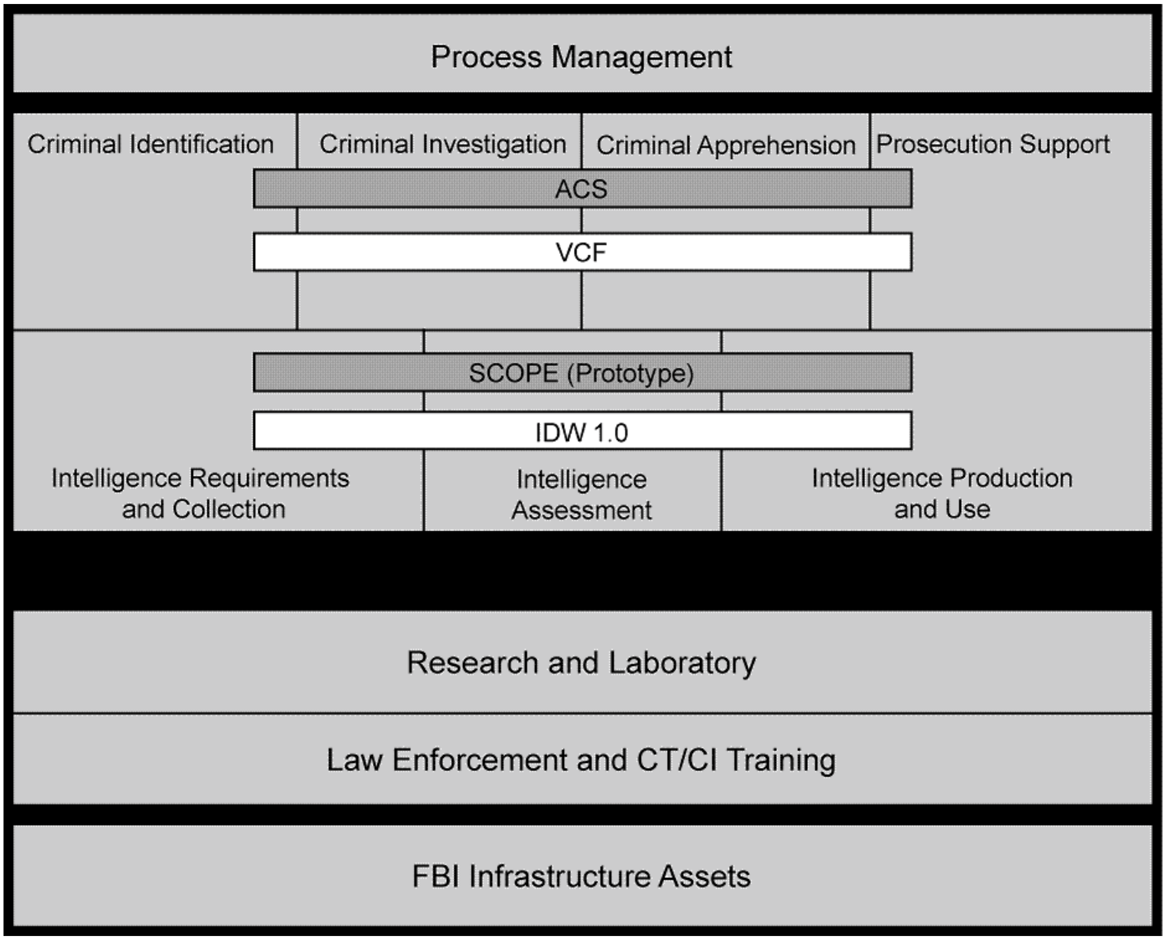

FIGURE 2 The scope of key applications on the FBI value chain. This diagram overlays on the middle portion of Figure 1 the FBI's currently existing IT systems (ACS and the SCOPE prototype) and the ultimate next-generation applications (VCF and IDW 1.0) and their purpose in relation to the bureau's core processes. Clearly, the FBI has hundreds of systems to be arrayed on a chart of this kind for it to be of most value. This task is not complex, and the results would greatly facilitate understanding both the "as is" and the "to be" contemplated by the Trilogy program and other FBI IT planning.

other words, the fact that the FBI was unable to present its own version of these figures was telling to the committee about a lack of clear architectural thinking. Without such a top-level description and understanding, all of the subsidiary steps in the design and implementation of an enterprise IT system are at significant risk of failure.

It is important for the FBI to create and use its own versions of Figures 1 and 2 to help explain its strategies, and to do the supporting work required to fill out their content. Once this is done, it does not matter if the FBI's own versions agree with the committee's figures, and a detailed acceptance or rejection of the committee's figures is not relevant.

The committee recognizes that the framework described above is only one way to conceptualize enterprise architectures. For example, the Federal Enterprise Architecture (FEA) framework,[5] to which the FBI has already committed itself, is used in many federal agencies. Multi-agency use of the FEA framework enables architectural efforts presented using its five-component framework to be directly compared across agencies. Nevertheless, the committee believes that the architectural triad described above is conceptually clearer and more straightforward than the FEA framework and that the FBI will make more rapid progress using the triad even if some translation between the triad and the FEA framework will likely be necessary at the end of the process.

Recognizing the Role of Top Management in Creating an Enterprise Architecture

An enterprise architecture has far more operational content than technical content. Accordingly, the FBI's enterprise architecture must be based on mission needs and must be formulated, propagated, owned, and evolved by the *operational* leadership of the FBI at the highest levels (the FBI director and the directors of the FBI's mission-oriented divisions).[6]

An effective process requires that the enterprise architecture be created by a combined effort involving both senior operational management and key technologists. The CIO plays a key role as the facilitator of the process; however, the creation of the enterprise architecture cannot be handed off to the CIO, and certainly cannot be outsourced. The enterprise architecture is central to an organization's strategy, as well as important for process analysis, change, and planning. Outside expertise can play a role in assisting and advising the enterprise architecture process, but the FBI's top management team must manage, buy into, and execute the process.

Although this task is critical, it need not be an enormously time-consuming one. With adequate time and focus on the part of senior operational management working with key IT people, major progress could be made in a week of intense work, and the creation of a reasonably complete operational architecture together with a top-level schematic systems architecture—the most critical part of the enterprise architecture—should be possible in a 6-month time frame.[7] Further, committee experience indicates that progress is best made with the top-level management team supported by an architecture team composed of a small number of full-time professionals *dedicated* to the task. These individuals must understand operations and have some appreciation for technology, rather than being technologists with only a loose connection to the operational side.

Given the fact that the leadership of any large organization, including the FBI, has many ongoing demands on it, the temptation is large to simply hire a CIO with a great deal of technology experience, delegate the task, and then forget about the problem. Why must an organization's operational leadership be deeply engaged in the development of an enterprise architecture for IT? Why can't this function be outsourced?

[5] The FEA is a business- and performance-based framework to support cross-agency collaboration, transformation, and government-wide improvement. See http://feapmo.gov/.

[6] In principle, it is also possible to begin with a vision of how technology might enable missions to be accomplished—that is, to seek a technology-driven enterprise architecture. But such an approach demands an extraordinarily high level of sophistication about the capabilities and limitations of technology, and for reasons that this report documents, is not appropriate for the FBI.

[7] The executive assistant director for intelligence testified to the committee that a small team working full time for about 10 weeks was able to develop a concept of operations for the Office of Intelligence. Thus, 4 to 6 months of work does not seem unreasonable for developing the operational dimensions of a larger enterprise architecture.

The committee's experience is that without the drive of operational missions, technology deployments inevitably serve to automate existing functions at a relatively low level, and thus the processes associated with these functions remain static. Even worse, automation of existing functions can degrade the ability of an organization to carry out its missions. The reason is that the functions that an organization must serve are sometimes in tension—consider an organization that must keep sensitive information secure (a driver for restricted access), and yet make it available to everyone with legitimate need (a driver for broad access).

When people deal with these competing demands, they make judgments and ad hoc decisions on the basis of their experience and expertise. Despite the existence of functional tensions in a non-automated system, human flexibility and adaptability generally ensure that operations can function at an adequate level of performance. Indeed, in most organizations, what people actually do on the job varies from what is specified by the organization's formal processes. These variances do not arise because people are poorly motivated or lazy, but rather because people are highly motivated, and the variances are usually necessary for real work to be done.

The fact that humans resolve these conflicts so smoothly, however, usually means that the tensions inherent in differing functions are hidden from view. Technology deployments bring out these tensions, and force someone to decide, in advance, how the tradeoff should be resolved. When automation is implemented in an organization without the benefit of operational knowledge (i.e., without taking into account what the organization is trying to do), the tradeoffs involved in deciding what to deploy are made in a vacuum—and often wrongly. Only the senior operational management is in a position to articulate explicitly how these tradeoffs should be resolved.

Beyond the need to develop an enterprise architecture to manage the IT investment process, it is important to recognize that the activity of developing an enterprise architecture often results in a (highly desirable) reexamination of operational processes. That is, by focusing on what technology can and should do for an organization, attention is naturally drawn to the processes it is intended to support—and often the processes themselves are seen to be outmoded, unnecessary, or ripe for streamlining, often because they were based on the limitations of older technology or on requirements that are no longer current. Such discoveries are valuable in themselves in that they help an organization function more efficiently even apart from its investments in technology. Such opportunities can be expected to arise when examining the processes of investigation and intelligence at the FBI.

Finally, as missions evolve, so must an enterprise architecture—and in that sense, an enterprise architecture is never final. Since it is only the senior operational leadership that can make basic decisions about the organization's missions, they will need to have a continuing involvement in the evolution of the enterprise architecture and a process to periodically revisit it. This point again reinforces the idea that an articulation of the operational dimensions of an enterprise architecture cannot be outsourced.

2.1.2 FBI Activities with Respect to Enterprise Architecture

Based on FBI briefings and presentations to the committee, the committee believes that the FBI's efforts and results in the area of enterprise architecture are late, limited, and fall far short of what is required. Indeed, in spite of the fact that the Trilogy projects are far along and substantial resources have been expended, the FBI has only very recently begun serious efforts to create its enterprise architecture, and no comprehensive enterprise architecture is in place today.[8]

For example, the FBI reported to the General Accounting Office that it has completed and approved an enterprise architecture "foundation document."[9] However, the FBI made no reference to this document or its content in its October 2003 and December 2003 presentations to the committee, despite its publication on August 23, 2003, and despite the fact that the committee raised questions about enterprise architecture many times during those sessions. Ultimately, the committee learned of this document by reviewing a DOJ inspector general report, and it obtained a copy of the document in early 2004.

Committee members have reviewed this document and believe that the document does begin to discuss at a high level some of the issues discussed above about linking the IT system to missions and operational processes. However, little follow-on work appears to have taken place as of the time of this writing (late March 2004).

In addition, the FBI has undertaken other efforts that could reasonably represent seeds of architectural work that needs to be done more broadly. The Office of Intelligence has embarked on a laudable effort to develop the beginnings of its own architectural sub-framework, and spokespeople from that office were able to relate IT requirements to operational process at a high level in a convincing manner. Those responsible for the VCF project have also developed an architectural sub-framework that appears adequate to support the initial rollout of the application in 2004. The VCF may well be a component that can be made, with some effort, to fit into the enterprise architecture when it is created. Nevertheless, these architectural efforts—important though they are—do not substitute for an overall architecture that addresses the missions of the FBI collectively.

The committee's concerns about inadequate enterprise architecture work are reinforced by the fact that only in the FY2005 budget enhancement request will the bureau include very substantial funding for enterprise architecture related activities, and that this request was under consideration at DOJ and the Office of Management and Budget (OMB) as of September 2003. (The FBI is further seeking to obtain an interim system engineering, integration, and test contractor to blend the Trilogy VCF, the Secure Counterterrorism Operational Prototype Environment (SCOPE), and the Integrated Data Warehouse (IDW), and several smaller efforts, into a unified and functioning whole.[10])

Under the best possible circumstances, this FY2005 budget enhancement request will take effect October 1, 2004, suggesting that FBI effort in this area will not be substantial at least until then. Moreover, the fact that this request has taken the form of a budget "enhancement" for FY2005 implies that the FBI has given this task a lower priority than might be implied, for example, by a request for authority to reprogram existing funds from FY2004 for this effort. In the absence of a serious enterprise architecture effort, even the interim plan to blend the VCF, SCOPE, and the IDW will be very difficult to achieve.

[8] In this regard, the committee's conclusion echoes the primary finding of the General Accounting Office report *The FBI Needs an Enterprise Architecture to Guide Its Modernization Activities* (General Accounting Office, GAO-03-959, September 2003, available at http://www.gao.gov/new.items/d03959.pdf).

[9] See Response of the FBI to the GAO report *The FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*, dated September 22, 2003. Available at http://www.gao.gov/new.items/d04190r.pdf.

[10] See Response of the FBI to the GAO report *The FBI Needs an Enterprise Architecture to Guide Its Modernization Activities,* dated September 22, 2003. Available at http://www.gao.gov/new.items/d04190r.pdf.

Beyond the lack of anything resembling a complete enterprise architecture, of most concern to the committee is the fact that most of the senior operational management of the FBI does not seem to have been deeply engaged in either the nascent architecture efforts or in shaping the Trilogy effort. For example, the *Enterprise Architecture Foundation Document* was produced by an entity called the Architecture Governance Board, whose members are apparently drawn from the FBI IT community—and did not include senior individuals from the major operational units of the bureau. That is, it does not appear to reflect substantial involvement by the senior operational leadership of the FBI and hence cannot be sufficiently complete to guide the FBI's IT development and deployment efforts.

This must change. For the IT modernization to succeed, frequent and engaged participation by the FBI's senior operational management in the creation and review of an enterprise architecture is necessary, and must be followed up with ongoing and systematic monitoring of the FBI's and contractor plans and progress through implementation. A properly designed process for developing an enterprise architecture can allow senior management to play their essential role without placing excessive demands on their time, and being actively engaged in the creation of an enterprise architecture does not necessarily mean that the senior operational management is responsible for every step. Rather, as the enterprise architecture is being created, the senior operational management must be involved in sessions at which there is serious discussion of the enterprise architecture's contents, and where important decisions are made. Many of these issues and decisions involve policy questions, including a determination of whether a relevant policy exists and thus should be reflected in the enterprise architecture, or needs to be created.

The committee believes that the absence of an enterprise architecture has been a major contributor to the problems faced by the implementers of the Trilogy program. That is, the lack of an architecture to guide the planning of an information and communication infrastructure has resulted in improvisation that has virtually no chance of resulting in a well-ordered infrastructure for the enterprise to build upon. In fact, merely providing parts (e.g., computers and accessories, piece-part applications, and so on) is like buying brick, mortar, and lumber and expecting a builder to produce a functional building without benefit of building codes, blueprints, or an understanding of how people will use the building.

2.1.3 Data Management Issues Arising from the Absence of an Enterprise Architecture

The FBI's lack of an enterprise architecture has manifested itself in many ways. For example, as noted above, the counterterrorism mission requires access to and the exchange of comprehensive and timely information. Thus, it is easy to imagine that the FBI will, under some set of circumstances, need to receive and/or send information from or to state and local law enforcement agencies (e.g., local police departments), its counterparts in foreign nations, or other members of the U.S. intelligence community.[11] The identification of precisely which

[11] A proof-of-principle project (the Gateway Information Sharing Project) was established in St. Louis in April 2002 to integrate investigative data from federal, state, and local law enforcement agencies into one database that will ultimately be accessible to all participating agencies via a secure Internet connection. The project merges investigative files and records from all levels of law enforcement into a single, searchable data warehouse, providing investigators and analysts the ability to search the actual text of investigative records for names, addresses, phone numbers, scars, marks, tattoos, weapons, vehicles, and phrases. The project is the result of cooperation between the FBI and a variety of state and local police departments in the St. Louis area and Southern Illinois. See DOJ press release of October 9, 2002, "Attorney General John Ashcroft Unveils Gateway Information Sharing Pilot Project in St. Louis, Missouri." Available at http://www.usdoj.gov/opa/pr/2002/October/02_ag_590.htm.

parties the FBI will share information with and the conditions under which information will be shared has profound implications for its enterprise architecture, and is an issue that the senior operational leadership must address.

A second issue is a potential confusion between mission and process. In discussions with the committee, senior FBI personnel repeatedly stated that "investigation and intelligence are the same thing." While it is true that the *mission* of criminal investigation makes use of intelligence *processes*, this fact does not mean that an IT infrastructure to support investigation should be the same as an IT infrastructure that can support intelligence. For example, the measure of success of an infrastructure that supports investigation is whether it helps agents to do their *investigation* more effectively, more efficiently, or with greater quality of output and national impact. Agents are the primary actors in criminal investigations, and they task analysts; thus, the developers of an IT infrastructure for investigation should regard agents as their primary customers.

By contrast, the mission of counterterrorism is intelligence-heavy. The measure of success of an IT infrastructure for intelligence is whether it helps the analyst *perform analytical functions* more effectively/efficiently, e.g., helps analysts identify patterns, clues, or other information generally indicative of events that have not yet occurred. In the intelligence process, analysts are the primary actors, in that they are the ones primarily responsible for analyzing a wide variety of information, from both open and classified sources, in order to identify impending terrorist actions that must be disrupted or pre-empted. Thus, agents will act on the information given them by analysts, and those actions are generally mapped into a criminal investigation. Presumably, agents also serve as collectors in the counterterrorism mission, and therefore can be tasked by analysts.

The following are some important differences that must be kept visible in designing IT support for the investigation and intelligence processes:

- Analysts tend to place a higher priority on access to a broad array of information resources, while investigators tend to place a higher priority on highly targeted information.
- Analysts may find "bad" or "untrustworthy" information contextually useful, while investigators may regard it as a liability and would want such information purged as soon as possible.
- Analysts must understand context and how a situation changes over time; investigators often place a higher value on information that can serve as evidence and fact.
- Analysts must handle and manage classified data, while investigators must generally, though not always, manage "law enforcement sensitive" or "sensitive but unclassified" data, which entails an entirely different set of requirements.[12]

In general, criminal investigation and intelligence are sufficiently different processes that the FBI would be wise to view the development of an overall enterprise architecture, particularly at the systems level, as calling for two subarchitectures with well-defined interfaces between them. An interface between the two subarchitectures is defined by the data that they exchange and share. These interfaces will require enforcement and oversight so that only

[12] There are exceptions to these generalizations, of course (e.g., investigations for counterintelligence purposes often generate classified information). But in any case, these exceptions represent only a small fraction of the total information collected.

necessary data are passed between them, and it will take senior operational management attention to define what data are "necessary" and what the policies are for the interface engines. Further, these interfaces have profound implications for the systems and technical architectures in areas such as standards that facilitate data exchange.

2.2 DESIGNING IT SYSTEMS TO SUPPORT FBI STRATEGY AND OPERATIONAL NEEDS

This section comments specifically on a few important applications design issues, including overall system structure; the design of data repositories; and workflow, security, and access, as well as a collection of specific deficiencies in the VCF and other applications. In most cases, these issues are a consequence of the lack of an enterprise architecture, and thus of the disconnect between enterprise architecture and technology planning and design.

2.2.1 The Virtual Case File Application of Trilogy

The Virtual Case File, the user application component of Trilogy, is a custom-designed software application that is intended to facilitate case file management by integrating data from older, separate investigative systems, including the Automated Case Support (ACS) system, and eventually replacing them. The VCF is intended to create efficiencies in entering case-related information by reducing the number of steps in filing documents and to facilitate the storage and retrieval of data for wider access, tracking, and analysis of case-related data.[13]

The VCF is a new IT application designed to be the primary operations system to support the investigative mandate of the FBI. The design process was under way prior to the addition of the intelligence mission, and the requirements for the intelligence mission were not included in the VCF design.

The VCF is a significant step forward from today's ACS system, and considerable progress on the VCF seems to have been made since September 2002. (The committee underscores the term "seems," because it was shown only a mock-up of the application, and not the application itself. That is, the committee viewed a canned presentation, because no working application was available at FBI headquarters. The committee notes that there is often a significant difference between the impression conveyed by a mock-up and what an actual application can do in practice.)

Perhaps the most important—and commendable—development in the VCF effort is the appointment of a very experienced and computer-savvy FBI special agent as program manager who has played a strong role in driving the design from user requirements. To the committee, this individual appeared eminently capable of articulating user needs based on operational experience rather than speculation, and the committee believes that it is this manager's operational insights that served as an implicit enterprise architecture (more precisely, a subarchitecture) for the VCF and that have consequently been a primary driver of significant progress. As such, the VCF has the potential to serve agents well in their criminal investigation mission.

[13] For further information about the virtual case file, see U.S. Department of Justice, Office of the Inspector General Audit Division, *The Federal Bureau of Investigation's Management of Information Technology Investments,* Report No. 03-09, December 2002, pp. 91, 94-99, available at http://www.usdoj.gov/oig/audit/FBI/0309/final.pdf.

Nevertheless, the committee is deeply concerned about certain aspects of the VCF effort. In the wake of the VCF prime contractor's failure to meet a critical delivery date for the Trilogy VCF component rollout,[14] the FBI has had to delay achievement of full system capability. In a memo delivered to the committee on February 11, 2004, the FBI noted that the revised schedule for Trilogy calls for achieving full system network capability (i.e., full functionality to 28,000 FBI employees at 612 sites) by April 30, 2004. Based on the VCF developer's original estimate that it would require 6 weeks of full system capability for testing the VCF, and assuming full system capability by April 30, 2004, it was estimated that the earliest activation of the first release of the VCF would be approximately mid-June 2004. Subsequently, the FBI advised that such an assumption would be incorrect given the level of immaturity of the VCF application delivered to the government in December 2003 and through continued evaluation of the application. The VCF vendor is scheduled to present to the government an estimated time to complete on April 8, 2004.

The details of the new VCF plan have not been made available to the committee. But in briefings held in October 2003, the FBI described to the committee a plan that would implement the VCF in what it describes as a "flash cutover." That is, the VCF would be rolled out for employee use all over the bureau simultaneously (or nearly so). The date for this cutover has been postponed, but the committee is concerned that, because of schedule slippage, the amount of testing will be reduced even further below what is already an inadequate level. With limited testing, and no experience gained from a limited initial rollout, the FBI would be implementing what amounts to a prototype throughout the bureau. This approach is nearly guaranteed to cause mission-critical failures and further delays, as discussed below in Section 2.3.1, with significant implications for training, performance, coherence, internal morale, public image, and cost to recovery.

The committee is also concerned that the VCF's current design and technical specifications lack the flexibility needed to incrementally improve the application to support additional functions important for the field agents and FBI management. This inflexibility will make further rounds of fixes and enhancements difficult. (Note that the comments below are based on a VCF mock-up in a canned presentation to the committee, rather than the committee's own exploration of a working VCF prototype.)

Based on the committee's understanding of and perspective on the VCF's current design, some of the potentially important issues related to the VCF include the following:

- As described to the committee by the FBI and its contractors, the current implementation of the VCF appears to have embedded the workflows describing how information is to be entered, reviewed, and used. Embedding the workflow in the application (that is, hard-wiring it) will make any such changes in the future much more difficult (more expensive and slower) to implement. Such changes are likely to be driven by changes in the operational processes that the VCF supports.[15]

[14] See U.S. General Services Administration press release, "Contractor Misses IT Delivery Date," November 3, 2003. Available at http://www.gsa.gov/Portal/gsa/ep/contentView.do?pageTypeId=8199&channelId=-13259&P=%7C40E6C831B9572449852568AF00594486&contentId=14244&contentType=GSA_BASIC.

[15] To illustrate how workflow changes might become necessary, note that FBI practices seem to be built around the assumption that only supervisor-approved documents have any status as information worthy of access by parties other than the original creator. However, in today's world of greater information sharing, an unapproved draft may well have information that might

- The VCF does not have an "offline use" mode. Without an offline mode, an agent working a case cannot take copies or extracts of case materials into the field for reference, nor create content offline that will then be synchronized into the VCF server when coming online. Today's administrative procedures may prohibit such practices, but if mobile computing and remote access for agents become desirable and necessary (as discussed in Section 2.2.4), the inability to access the VCF in an offline mode will become critical. Remote operation, whether offline or via a communications link, has proved to be a major enhancer of productivity in a wide variety of situations.
- In the VCF, documents are indexed with terms that are manually specified by supervisory agents without any auxiliary capability for the automatic generation of index terms. Manual indexing reflects today's practice in the FBI, but modern indexing software can do a very good job of finding index terms in a corpus of text automatically. Manual indexing will fail to supply terms that are outside the context of the human indexer, as many counterterrorism activities are likely to be. Today, full-text index systems that index every word in a document are the foundation of powerful search engines, such as Google, and are being exploited to a higher level in extracting meaning automatically in some experimental systems. It is true that basic automatic indexing systems are unable to provide index terms that are not explicitly represented in the text; for this reason, automatic indexing is not a replacement for manual indexing as much as it is a very fast and powerful supplement for it.
- The VCF appears to lack broad automatic notification of changes that are made. Case owners are made aware when documents are added to a case file, but no other parties are notified. In an environment in which many people (investigators and analysts) may use a case file, such lack of notification places a large burden on those users to check the contents of the case file periodically. They will waste time in checking a file that has not been altered and lose currency between the point of update and their access to the file. Lack of notification is thus an inhibitor of collaboration.
- The VCF appears to lack useful capabilities such as bookmarking, favorites, or history features for an individual user. Without such features (commonly available on most Internet browsers), users are poorly equipped to remember where they are or where they saw interesting information. This fact is particularly significant when the volumes of information with which one is working are large. Such capabilities would be useful now, but will be expected by any user in the future.
- The VCF appears to be weak in its ability to sort data. The ability to sort columns of names or dates or other such information is quite valuable when one has only a vague memory of a name or a date associated with it. For example, a user may remember that a document was from the June 2001 time frame. If the system does not allow a sort by date, the user is forced to search explicitly for all documents dated June 2001. This does not appear to be a drawback, until one realizes that his memory may be incorrect, and in fact the document appeared on May 31. By arranging the entries according to date, the user can rapidly scan both sides of the putative date index, and the negative impact on information retrieval of errors in recollection can be reduced.

prove useful to another agent or to another case, and procedures may need to be changed to accommodate a different sharing arrangement. Other examples might be the need to cope with shifting organizational structure and roles, or with new missions and legislation or regulation.

- The VCF interface presented to the committee was inconvenient in some respects. For example, the committee saw no evidence that hot links to organizational and user information were provided, even though such information could be supplied easily. To increase the VCF's convenience, a case file should have listings of everyone who accesses the file and should provide online contact information about those users to facilitate contact.

One might draw an analogy between the VCF and "blogs" (i.e., Web logs). Today, members of the Internet community often use blogs to observe and comment on some theme, or to discuss various topics. The VCF captures observations about a case, and may include a commentary describing the investigator's reasoning. Some blogs support cross-referencing and commentary by contributors other than the primary author. The VCF, particularly when seen through an analytic lens, might benefit from richer discussion and content, dynamic cross-referencing of cases, and external commentary on the reasoning behind a case or cross-references. The culture of blogs and the technology to support them may provide a rich source of external ideas for the future functionality of the VCF, as well as commercial technology for future implementations. An example is the Really Simple Syndication protocol used with blogs to notify interested parties of changes, thereby eliminating the need to constantly revisit a blog to understand what has changed.

All of the above issues can be addressed in subsequent releases of the VCF. A more staged rollout of the VCF would likely have resulted in more focus being put on these and other still-to-be-identified shortcomings. The VCF will certainly require ongoing multiple releases, and it is essential that the FBI substantially enhance its capabilities in design and implementation for these ongoing investments.

2.2.2 Data Management and the Integrated Data Warehouse (IDW)

The FBI has a tremendous quantity of data, most of which comes from its investigative processes. This data must be organized and managed in a way optimized to promote the effectiveness of the bureau's agents and intelligence analysts. Access capabilities required for intelligence analysis to determine possible events in the future often differ greatly from the access capabilities required for reliable case records management, which has the mission of organizing and retaining information to meet rules-of-evidence requirements. Accordingly, because it need not follow rules of evidence, the intelligence process may have different trust models governing browsing of information.

Thus, the information requirements of the investigative and the intelligence missions of the bureau are very likely to require very different work processes and information access. It is very likely (nearly certain) that different data models will be required in order to provide efficient support for these separate missions. Furthermore, each mission of the bureau has unique constraints for access to the information and will require different security models and different tradeoffs between security and accessibility. Implementation of these models is likely to show that distinct systems, with overlapping contents and interface engines to manage data sharing and inter-organization handoffs, will be needed to assure manageability in the presence of conflicting constraints.

The Integrated Data Warehouse (IDW) will serve as a repository to store external data from a variety of sources that come into the agency at different frequencies, such as criminal information from other government agencies and visa data.[16] The IDW will remain separate from the VCF but will replicate much of the data in the VCF. With proper security and sharing rules placed on the data, the IDW is intended to allow teams of analysts and agents to run queries horizontally across the data, and to share subsets of the data with other government agencies.[17]

According to briefings to the committee, the IDW is intended to be a resource for intelligence efforts (among other roles), and to be used by FBI analysts and shared with other intelligence agencies. For such analyses data from non-FBI-sources will have to be included in the IDW.

These briefings also suggested that data modeling efforts for the criminal investigation mission were just getting started. Further, the data models of the IDW presented to the committee (and the VCF for that matter) were far too abstract to be very useful, though the presentation from the intelligence side recognized that there were differences in need between the investigative and intelligence analysis functions.[18]

Three examples will suffice to illustrate a disconnect that needs to be resolved between the data models as described to the committee and operational needs:

- Presentations to the committee raised the issue of data currency. That is, intelligence analysts seemed to expect to have access to live databases containing the most current information, while the design of the FBI's data warehouse incorporated copies of production databases. If the warehouse is intended to contain copies, the issue is raised concerning the frequency at which the warehouse copies are refreshed from production databases.
- The IDW appeared to have been designed to overwrite old copies of databases with newer copies, so data can be there one day and not the next (that is, the IDW is not equipped to handle time-series of versioned data). While having only the most recent copy of data may be appropriate for the purposes of an investigation (presuming the most recent copy is the most accurate and reliable), this assumption is almost certainly not valid for intelligence purposes.

[16] The committee notes that the IDW acronym itself is subject to some confusion. Director Mueller has made reference in congressional testimony to an "*Integrated* [italics from the committee] Data Warehouse [that] will link 31 FBI databases for single-portal searches and data mining." The DOJ inspector general report states that "the FBI expects to use the network to transport the *Investigative* [italics from the committee] Data Warehouse, which will link 31 FBI databases for single-portal searches and data mining," and the FBI briefed the committee on IDW referring to the "Investigative Data Warehouse." Whether this inconsistent use of the acronym is inconsequential or reflects a deeper confusion within the FBI about the purview of data to be contained in the IDW remains to be seen. For Mueller's testimony, see http://www.fbi.gov/congress/congress03/mueller032703.htm; for the DOJ IG report, see http://www.usdoj.gov/oig/audit/FBI/0336/exec.htm.

[17] Robert S. Mueller III, "Congressional Statement on Federal Bureau of Investigation's Fiscal Year 2004 Budget," House Appropriations Committee, Subcommittee on the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies, March 27, 2003, available at http://www.fbi.gov/congress/congress03/mueller032703.htm.

[18] Data models are generally used by system architects and designers in an iterative refinement process that starts with a conceptual data model, which deals with the key business concepts of the database, and then proceeds to a logical data model, which allows designers to reason about the primary relationships among the key data tables and elements, and then finally ends up with a physical data model, which documents the database implementation details. Modern computer-aided software engineering tools often facilitate the refinement process, reducing the labor required to construct and manage the three levels of model. Rather than include any specific recommendations about data modeling, the committee notes that the FBI's enterprise architecture effort should identify a data modeling framework to be used by developers and implementers. An essential element of data modeling is a data dictionary, which defines the basic structure and organization for the database with which it is associated. The construction of data dictionaries for the various databases is an essential prerequisite for sharing data between databases.

- Some of what was presented when the committee asked about data models were not data models at all, but rather hierarchical XML descriptions of various criminal justice documents (e.g., arrest forms, booking reports, sentence orders, and so on).

To illustrate what a high-level enterprise perspective on data management might entail, consider that IT systems for the FBI must serve multiple operational functions. From the committee's perspective, the major classes of data are data to be kept in:

- The active case records used by the field agents—these are to be served by the VCF system under development.
- A broad-based data warehouse to serve intelligence tasks now assigned to the FBI—these were served by the SCOPE prototype demonstration and are to be served by the IDW follow-up projects.
- A reliable repository of record that will provide a formal backup source for prosecution of criminal cases, intelligence investigations, and internal audits. It is restricted to holding data for which the FBI is formally responsible. As such, it will be smaller, less visible, and more stable than other FBI data systems, will be highly reliable and capable of becoming the FBI's replacement for paper documentation, and will spare other FBI IT systems some of the more stringent requirements that can inhibit their operation.
- A wide variety of management and administrative databases for personnel, capital and registered item inventory, evidence tracking and inventory, and so on, to allow FBI headquarters to carry out its responsibilities.

Data in each of these classes are not entirely independent of each other, and thus applications to manage these types of data must have linkages among them. (For example, information related to a given legal discovery motion or Freedom of Information Act request may be contained across these different types.) In addition, there may well be linkages to data contained in databases operated by other agencies (e.g., data supporting FBI intelligence tasks may well originate in databases operated by the CIA). However, the fact that the applications must have linkages among them does not mean that the databases must be co-located or should be managed by the same staff under the same access rules—a point especially likely to apply to data-linking connections to intelligence agencies.

To understand fully the high-level requirements for these applications, their objectives must be made explicit. Based on what it learned from the FBI about its data handling needs, the committee infers the following list of objectives for systems that handle each major class of data described above.

The VCF should:

1a. Serve the field agents and their supporting analysts, wherever they are, in tasks of information collection and analyzing the collected information on their cases.
1b. Be available 24/7.
1c. Allow convenient upgrading of services as needed by the agents and enabled by technology.
1d. Provide linkages to data in the IDW and other FBI databases, and allow insertion of records from other sources that have been determined to be pertinent to a case by the responsible agent and his/her supervisor.

1e. Purge closed cases, but keep track of them for analysis purposes.
1f. Keep all the information secure vis-à-vis outsiders (i.e., outside the FBI).
1g. Keep some elements secure vis-à-vis most FBI personnel.
1h. Be flexible enough to accommodate changes in operational processes that may be made in the future.
1i. Resist tampering with records.
1j. Support an appropriate degree of auditing when information is entered or changed.
1k. Support audits for system use (a security measure). (System use refers to read access, write access, and search results.)

The IDW should:

2a. Serve broad intelligence functions of agents and analysts.
2b. Acquire, integrate, and store data from other sources of potential relevance for broader analyses, such as sources from the Department of State, Immigrations and Customs Enforcement, and foreign sources.
2c. Allow mining of information that is not (yet) related to a specific case within the time that might be needed to mobilize a team to respond to an incident (say, within 20 minutes). (This time appears to be an achievable goal with current technology for obtaining and integrating data from known remote sources.)
2d. Have the capability to store tentative conclusions, and to purge such information if it is determined to be misleading.
2e. Be flexible to support an increasing variety of data mining and analysis tools to be installed as they are found to be useful.
2f. Protect its content so that it is secure vis-à-vis outsiders and unauthorized insiders or turncoat insiders.
2g. Not contain information that would be forbidden to any FBI personnel.
2h. Support an appropriate degree of auditing when information is entered or changed.
2i. Support audits for system use (a security measure). (System use refers to read access, write access, and search results.)

The repository of record should:

3a. Serve broad intelligence functions of agents and specialized, authorized personnel, including internal audits.
3b. Serve legally required documentary archival storage requirements, with complete audit trails, primarily to provide backup for cases under prosecution or review, including sensitive information that would be unwise to have available within systems that allow broader access.
3c. Maintain extremely high reliability and integrity, even at the expense of 24/7 availability and flexibility.
3d. Be fed primarily from the VCF, and exclude material that is not the responsibility of the FBI.
3e. Support tools used solely for records management and not for investigation or analysis. (That is, only tools for records management should be run against the data in the

repository of record, though the contents of the repository of record may be an input to a larger pool of data that can be analyzed with arbitrary tools. Thus, the data models of the repository of record should be developed in a way that anticipates this use/interface.)

3f. Be reorganized only rarely.
3g. Not be used as a working resource by FBI personnel.
3h. Be maintained at a very high level of security.
3i. Support appending of contents rather than record purges for updates.
3j. Resist tampering with records.
3k. Support an appropriate degree of auditing when information is entered.
3l. Support audits for system use (a security measure). (System use refers to read and write access.)

Administrative databases should:

4a. Serve a variety of FBI management and administrative functions.
4b. Be maintained and updated primarily by FBI personnel at headquarters.
4c. Be accessible to field personnel for determining the location of their colleagues, resources, and equipment.
4d. Manage the operational security issues associated with making such data available (in 4c).
4e. Be available at close to a 24/7 schedule, although updating of information may be constrained to business hours.
4f. Be secure vis-à-vis outsiders.
4g. Not contain information that would be forbidden to any FBI personnel.
4h. Evolve to align with Department of Justice standards for administrative support systems (e.g., finance, e-mail).
4i. Support an appropriate degree of auditing when information is entered.

The FBI may disagree with this listing of essential objectives, which the committee has created based on limited knowledge and in the absence of an FBI enterprise architecture. Agreement in detail is unimportant, but the FBI *must* develop its own list of essential objectives, including priorities, tradeoffs, and explicit analyses, based on its own understanding of its essential operational processes and how it expects to use these databases. In any event, the diversity of requirements makes it clear that these storage applications must be implemented in separate systems, and that different policies will be needed to ensure the proper balance of accessibility, security, availability, and reliability.

It is likely that there will be a fair amount of duplication of contents in these databases. However, the cost of replicated storage is less than the cost of the manpower needed to maintain a single complex system with multiple and potentially contradictory objectives. Replication also mitigates some security problems, such as denial-of-service attacks (see Section 2.2.5). With multiple copies, there is also a significant probability of inconsistent or out-of-synch information. This is especially true with information that can change over time. Cleaning and validating information will become a separate process unto itself.

The IDW has a broad role, and correspondingly broad objectives and access needs.[19] The committee understands the intent behind the broad access needs of the IDW and other systems for managing operationally relevant data, but from a pragmatic standpoint, it will be difficult to design a single system to meet these access needs while still retaining necessary security measures.

Consider, for example, the statement that "the ownership of FBI information is corporate; no individual division or employee 'owns' FBI information." Such a principle is attractive, for entirely understandable reasons. But the agents who collect the data will undoubtedly be concerned about maintaining control over data distribution and protection of sources and methods. Today, these issues are managed through informal information-sharing networks of agents and analysts that operate not only on the basis of formal access control provisions such as level of security classification but also on personal knowledge and trust of the individuals involved.

Information management systems that do not provide these agents with some control over the release of certain kinds of information may increase the likelihood that important information may not be entered at all. Agents or other information collectors may be inclined to keep two sets of records—one for official use and one for more sensitive information, allowing them to maintain control over the disposition of sensitive information.

This record-keeping challenge, whether based on realistic concerns or perception, is unlikely to be overcome by fiat. That is, a directive that agents and other collectors record officially all information, regardless of the sensitivity of its source, is likely to be quietly disregarded in many instances. Such disregard would not necessarily be gratuitous, but rather an entirely understandable reaction of collectors in the field who might be reluctant to trust the security of their sources to another party.

2.2.3 SCOPE

The FBI demonstrated the Secure Counterterrorism Operational Prototype Environment (SCOPE) to the committee. This demonstration illustrated the analytic tool suite with synthetic data. The analytic tools were based on commercially available products that included support for data visualization, relationship analysis, and automated language translation. Because this demonstration was not done using operational data or the Trilogy network, the committee cannot comment on the performance or scalability of this approach.

[19] For example, a July 2003 draft Integrated Information Sharing Plan lists the following eight guiding principles that the FBI expects to apply to its information-sharing strategy.

- All FBI data is to be shared within the FBI, with very few exceptions.
- The ownership of FBI information is corporate; no individual division or employee "owns" FBI information.
- The FBI will have a single, integrated information space, in which the default will be to share with agencies with due consideration for the protection of sources and methods, and the security and prosecutive objectives of investigations.
- The FBI will not filter information internally but instead will create an overarching FBI-wide policy that balances the need for cross-correlation with the risks of misuse.
- The view of what the FBI collects and what the FBI creates will look very similar.
- All data collected must also be recorded, searchable, retrievable, and easily cross-correlated.
- FBI employees will have the ability to conduct federated queries across multiple systems to identify relationships.
- Technology will be in service of people instead of people in service of technology. The FBI must have interconnectivity with Intelligence Community systems. Additionally, the FBI must leverage existing technologies instead of rebuilding them.

The committee did not review this draft plan. The text above is contained in a DOJ Office of the Inspector General report, *The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information*, Report No. 04-10, December 2003, available at http://www.usdoj.gov/oig/audit/FBI/0410/findings2.htm.

The committee believes that the FBI has an important opportunity with SCOPE. Here, the FBI is not burdened by a legacy of analytic tools and data models. It has a unique opportunity to assemble and integrate the most promising analytic ideas and tools. A well-conceptualized enterprise architecture and data models are critical to successfully exploiting this opportunity and creating an environment that can incorporate the best analytic ideas and products over time. (This point reinforces the immediate need to develop and understand the data models and the workflow.)

The FBI's use of commercial products is laudable. This willingness to look beyond conventional sources for the best available ideas can provide the FBI with an analytic advantage. The commercial market for such tools is being driven by much broader trends than just counterterrorism. These trends include the private sector's desire to analyze and support market data, and the increasing globalization of markets. By harnessing the commercial market for analytic tools, the FBI can gain access to far more creativity than it could ever capture with internally developed tools.

Commercial products can also be expected to incorporate the best practices in human-computer interfaces. Even if the FBI does not use commercial tools, it should study their human-computer interfaces and incorporate the best ideas into the tools it develops internally. An approach rooted in commercial products does not rule out one-of-a-kind tools that are internally developed.

2.2.4 Mobile Computing

The FBI's interest in wireless data communications appears to be driven primarily by operational continuity considerations. For the most part, the FBI's experience with wireless data communications has been through personal digital assistants (PDAs) used by a small number of senior leaders. Anecdotal reports suggest these individuals have found that wireless data communications enhance the conduct and accelerate the pace of day-to-day business.

To make further progress in this area, the FBI is planning a trial of PDAs at a field office. Such a trial can be the basis for establishing a baseline characterization of agent and other activities in that office to understand if the deployment of PDAs has any impact. Thinking about how to create a baseline characterization of office activities, which in the future might involve mobile computing platforms such as PDAs or laptop/tablet computers, can also contribute to quantifying an office's implementation of the FBI's operational processes that are the critical input to the FBI's enterprise architecture. The planning and results of this trial should be coordinated with the FBI's enterprise architecture efforts.

2.2.5 Security

Loosely speaking, the security of an information system or network refers to its ability to continue to support authorized parties when it is under attack and its ability to resist the efforts of unauthorized parties to compromise its operation or data. For this report, it is helpful to conceptualize security issues along two dimensions—those that arise from the disconnect between the FBI's operational mission needs and its enterprise architecture, and those that arise from inadequate thought about the implementation of whatever security policy is adopted.

The disconnect between the FBI's operational mission needs and enterprise architecture is reflected in the FBI's expression to the committee of a philosophy of zero tolerance for security risk, seeking not to manage risk but to avoid it. Given that the FBI's information systems are prime targets for criminals, espionage organizations, saboteurs, and terrorists (some possessing significant technical and human resources), the sentiments underlying this view are quite understandable. Nevertheless, the only approach that truly provides *zero* risk is one that destroys all information as soon as it is collected or that otherwise makes information entirely inaccessible to anyone.

A zero tolerance for security risk is doubly problematic in an environment in which information must be shared. There is a deep and unavoidable tension between information sharing and information security, and while there are mechanisms that allow design architects to mitigate this tension (a matter of implementation discussed below), some tensions are unavoidable, and at some point the senior leadership must decide what degree of security risk is acceptable and under what circumstances in return for the advantages of broad-based information sharing.

For example, it is the committee's understanding that agents and intelligence analysts are not routinely provided with Internet access for security reasons. It is certainly true that a lack of Internet access will prevent Internet-based security compromises, but it also impedes the use of the Internet to search for potentially valuable publicly available information. (For example, FBI agents assigned to field divisions without Internet access must go to public libraries to search the Internet, and must use various commercial e-mail accounts.) This is a reasonable policy only under the implicit assumption that publicly available information is not useful in either intelligence or investigation—and this assumption is simply not tenable for the counterterrorism mission.

Furthermore, isolating FBI staff from the Internet precludes their being educated by casual exposure to the best new ideas and tools emerging in the global Internet community. While there are individuals with deep expertise, often gained by dedicated people spending their own time and money, and there are specific provisions for controlled access to the Internet, there is no substitute for the institutional and cultural impact of broad availability of Internet access to all FBI staff.

Another important issue with profound consequences for security is raised by the attempt to make a single physical IT infrastructure serve the needs of both intelligence analysts and law enforcement investigators. Much intelligence information is classified, with rigid security requirements imposed by legal and national policy. However, much of the data related to investigations is unclassified (sensitive but unclassified (SBU) or law-enforcement sensitive). Devising technologies and policies to manage both kinds of data under one rubric is thus potentially contradictory, unless one is willing to accept the severe operational penalties of treating unclassified information (SBU or law-enforcement sensitive) as classified.

Intelligence analysts also have a need for relatively unfettered "browsing" through information. However, sensitive information (e.g., identities of informants) can be derived or deduced from aggregation and inference from large amounts of apparently unrelated data.

There are ways to manage these tensions, such as allowing intelligence analysts access to "pointers" to protected internal information rather than the information itself, so that the analyst can make a direct request for access to the party responsible for protecting that information. In the area of unclassified versus classified data, it would help to attempt to balance the threat of misuse or inappropriate access against the benefits of allowing more use, e.g., by remote agent access in the field; this process is known as a risk management assessment. Nevertheless, the tension cannot be eliminated, and only the FBI's senior operational management is in a position to judge how this tension should be resolved.

A third security tradeoff will manifest itself when mobile computing becomes an issue. The value of mobile computing is likely to be high, but mobile computing is inherently more vulnerable than office-based computing, and the senior operational leadership will have to decide if the increased security risks are worth the added operational flexibility. Empirical data and a formal evaluation process for mobile computing would be useful inputs to the leadership. The FBI's PDA experiment will help the leadership to think through how to differentiate and measure communications that involve classified information, SBU information, and unclassified information, each of which has different security requirements.

In the absence of any specific information on the subject but based on previous experience, the committee suspects that a significant fraction of, if not most, FBI data communications traffic need not be carried at the classified level. If the measurements associated with a PDA trial support this conjecture, the FBI may be in position to take advantage of wireless data communications in designing an infrastructure, systems, and processes to implement its enterprise architecture. Such systems and policies could differentiate between SBU and unclassified communication, handle them differently, and significantly improve FBI metrics for efficiency and effectiveness. If this conjecture turns out to be true, the FBI would also have to establish a clear policy governing SBU communications.

The committee is also concerned about a number of security issues related to implementation. These include:

- *The use of passwords for authentication*. The weaknesses of passwords as an authentication mechanism are well known (e.g., they are easily compromised without the owner's knowledge),[20] and yet no thought seemed to have been given to alternatives.
- *The lack of consistent security models between the IDW and the VCF*. In particular, this inconsistency suggested that searches of data contained in the VCF from the data warehouse side would not be made visible to case owners. Moreover, as long as security mechanisms only provide access control, and do not log the information that is accessed, then misuse of systems by authorized users will not be visible until the information turns up in the wrong places. (And, of course, logs must be reviewed regularly by automated log analysis tools supporting human analysts.)
- *The operating system monoculture*. The Trilogy IT modernization put into place a single operating system environment, and the security vulnerabilities of an operating system monoculture are well known.[21] Such an environment carries with it the risk that a single exploit, such as a worm or virus, can result in global failure of the Trilogy network.[22] The technology

[20] See, for example, Department of Defense, *Password Management Guidelines,* April 12, 1985, available at http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.html.

[21] National Research Council, *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, Computer Science and Telecommunications Board, National Academy Press, Washington, D.C., 2002.

[22] Note also that security risks may be especially great during a time of transition between old and new systems. The reason is that anomalous system behavior can have multiple causes, and may reflect operator inexperience, inherent system bugs, or adversary-planted exploitation. Uncertainty about the actual cause may lead to inaction for a longer period of time than would be the case during normal operation.

deployment plan relies on isolation from the Internet and diligent network monitoring and response to protect against such problems. But neither of these approaches, taken singly or in combination, can eliminate the risk of catastrophic failure, and recent worm/virus experience has shown that self-propagating, malicious code can enter isolated networks through an unwitting laptop user connecting to the isolated network after having been connected to, and infected through, the Internet. Furthermore, the propagation speed of modern worm/virus code is sufficiently rapid to overwhelm any monitoring and response center staffed by humans.

- *Seemingly inadequate contingency plans for operating under attack*. A basic principle of managing a critical operational network is that plans for maintaining operation in the face of a compromised element must be made in advance.

  —How are nodes in the network protected against other nodes that may have been compromised? Rather than a simple perimeter defense, a principle of mutual suspicion should apply that does not allow an attacker who has breached the perimeter to have free access to the entire network.[23]

  —How will the FBI's public-key infrastructure be managed in the face of an insider threat?

  —How will key revocation be handled? Emergency re-keying? Access overrides (i.e., how will authorized parties obtain access if access tokens and/or information are lost?)

  —How will worms and viruses be purged from the system if they are introduced?

  —How will the network respond to a denial-of-service (DOS) attack? There are many different flavors of DOS attacks, ranging from a deliberate attack on the inside of the network to an attack occurring on the "outside" of the network that merely consumes bandwidth and degrades the performance of the public links that carry the virtual private networks of the FBI.

- *Missing or incomplete validation of a security architecture*, which the committee inferred on the basis of presentations to it. Specifically, the FBI did not provide to the committee evidence that it had validated:

  —The putative design principle for security, which seemed to be characterized by an approach of "build to DISA (Defense Information Systems Agency) gold standard and back off until tools work."

  —The model of the threat that faces the FBI's IT systems. (Note that a threat model must include threats emanating from both inside and outside the organization.)

  —The use of the electronic key management system developed by the National Security Agency (NSA) in the context of the specific needs of the FBI.

In each of these cases (the design principle, the threat model, the use of the NSA electronic key management system), the approach may be plausible and ultimately desirable. But a process of systematic validation is necessary before those conclusions can be drawn. More generally, a security architecture is based on an understanding of the data flows in the organization (derived from the enterprise architecture). Based on these data flows, the databases that need to be isolated are identified. When necessary, controlled interfaces between isolated and non-isolated databases are also identified. These interfaces are then mapped onto the physical network configuration to decide what links/nodes must be encrypted, physically protected, or both. Lastly, the security architecture requires both a plan for managing encryption keys and a vulnerability assessment (i.e., a paper attack on the paper architecture).

[23] To illustrate, this principle might call for the use of firewalls on every node of the network and anti-virus protection running continuously on all computers connected to the network to mitigate denial-of-service or intrusion risks.

- *Potentially inadequate proactive counterintelligence against inappropriately trusted insiders*. As the Robert Hanssen case illustrates, security must be maintained against deliberate exfiltration of sensitive or classified information. Counterintelligence tools for this problem include logging of access, analysis of logs, and possibly filtering of outgoing information. Note also that notifying the owner of a sensitive information item that some other party has accessed that information is a potentially powerful way of raising red flags.
- *Potentially inadequate security of hardware and software implementation*. When hardware is deployed and software is written by outside contractors, there are greater risks that hostile parties working for the contractors may seek to insert trapdoors and other ways of bypassing security in the systems being deployed. As a general rule, these risks can be managed, but the weakness of the FBI's contract management abilities may mean that the FBI's efforts in this area are not up to par (e.g., as with Defense Department special access projects). The same considerations apply to commercially acquired infrastructure software. Though it might be difficult for an attacker to compromise a component of such software, the possibility cannot be ruled out. Moreover, even security patches and upgrades are not always guaranteed to work properly, which means that installation of such upgrades cannot be undertaken blindly or without explicit thought from IT-savvy managers.

2.2.6 Privacy

As part of the FBI's briefings to the committee, the FBI's privacy office addressed the committee, from which the committee concluded that the FBI did have some sensitivity to some of the relevant privacy issues. However, the committee has not undertaken a comprehensive study of protection of individual and corporate privacy in the context of the FBI's IT modernization program, and thus the comments below can only suggest some of the issues that may be involved.

- The FBI must proceed with great sensitivity to privacy issues as the counterterrorism mission assumes greater importance, and both substance and perception are important in this domain.
- There are many substantive issues associated with privacy. For example,

  —The FBI privacy office seemed to the committee to be geared primarily to protecting personally identifiable information from being improperly shared outside the FBI (e.g., with contractors), and in the short presentation to the committee, its approaches to this problem seemed reasonable.

  —Another privacy issue not addressed in briefings but of great concern to the privacy-sensitive segment of the public is the protection of the public from the abuse or improper use of such data by rogue FBI employees acting on their own or through some official though perhaps not publicly acknowledged FBI program. The committee has no comment on this issue, other than noting that the simple exhortation "trust us" is not likely to be reassuring to this segment even if in fact the FBI is doing everything possible to prevent such abuses from happening.[24]

[24] Note also that Section 223 of the USA PATRIOT Act allows individuals to recover monetary damages and litigation costs from the United States in the event that information or records are willfully and improperly disclosed, a fact that increases the importance of keeping good records of who is accessing what data and under what circumstances. In addition, federal employees found to have improperly disclosed information are also subject to administrative action under the PATRIOT Act.

- Perception is at least as important as substance. That is, a technically well-conceived privacy protection program solves the substantive problem. But even with such a program in place, the FBI must also pay attention to external perceptions, because those are a major influence on the public trust that the FBI must maintain in order to be effective.

2.3 ENSURING EFFECTIVE MANAGEMENT OF IT DEVELOPMENT AND IMPLEMENTATION

This section addresses a variety of serious management issues in the FBI's IT modernization program. Issues and problems identified here relate to the management approaches and processes used by the FBI across the implementation life cycle, including requirements determination, development methodology, contracting and project management, system rollout, training, evaluation, and metrics of effectiveness. While the committee's comments regarding implementation are derived from its consideration of the Trilogy infrastructure and VCF projects only, the committee believes that dealing systematically with these issues is essential to success in follow-on efforts such as the IDW and SCOPE.

2.3.1 Overall Development Methodology

In the committee's judgment, the FBI's management approach to the Trilogy modernization violates a number of basic principles that should govern the development of large systems.

Principle 1: *Any organization that depends on the continued operation of its IT systems and is modernizing those systems should plan on the simultaneous operation of both old and new systems for some period of time, so that failures in the new system do not cripple the organization*.

Large-scale deployments involving new technology almost always come with problems (e.g., system crashes, unacceptably slow performance), and there is some risk that the problems will be so severe as to prevent the effective use of the entire system for some period of time. Accordingly, there must be backup and contingency plans in place that anticipate a wide range of failure conditions. However, the committee saw little evidence that such plans had been formalized, and indeed has been informed that the current transition plan does not envision the availability of the ACS after the cutover to the VCF, even though the hardware supporting the ACS is neither being redeployed to support the VCF nor being immediately decommissioned.

Effective transitions are usually managed gradually. Even where the transition is abrupt, maintaining the function of the old system for some period as a fallback option is good practice. Any ACS-to-VCF transition without a backup plan is far too risky for the FBI and for the nation, especially in light of the FBI's myriad and critical operational responsibilities to the nation that will continue during any such transition.

The costs of maintaining a fallback plan and a supporting infrastructure are small compared to the operational costs associated with large-scale VCF problems. Moreover, because the hardware supporting the ACS will not be converted to support the VCF, there is a residual and pragmatic disaster-recovery capability to revert to the ACS. But contingency plans that anticipate a continuing if temporary need for the ACS must be made *before* the transition to exploit this residual capability, or else the use of the ACS in this contingency mode will suffer.

Expenditures to maintain an infrastructure that can support concurrent use of the ACS and the VCF for a limited transition period would be a worthwhile insurance policy.

Principle 2: *Any organization undertaking a large-scale IT system development and deployment, but especially an organization without a strong track record in IT development and use, should develop, test, evaluate, and iterate a small-scale prototype before committing itself to an organization-wide program.*

The development methodology for Trilogy seems to be based on a one-way non-iterative process where rigid specifications are generated in advance. Subsequent changes can then be argued to be "specification changes" that open the door for schedule delay and increased expense. In truth, it is essentially impossible even for the most operationally experienced applications developers to be able to anticipate in detail all of the requirements and specifications in advance. Therefore, development contracts should not make such an assumption, but rather should call for an approach to specification of user requirements that is based on a process of extensive prototyping and usability testing with real users.[25]

To the best of the committee's knowledge, apart from SCOPE, no prototype has been developed for any of the major components of Trilogy (the Trilogy network or the VCF) or for the IDW. As the FBI recognized in developing SCOPE, the advantage of a small-scale prototype is that it can be iteratively developed with strong user feedback and involvement, thus increasing the chances that what is ultimately delivered to the end users meets their needs. This point is relevant to many dimensions of system development, including the functionality desired in a new application, the convenience and intuitiveness of a user interface, and the nature and mix of the operating load that the system must support under real operational conditions.

In some instances, the intimate involvement of project managers with extensive operational experience can play an important role in some of these dimensions (e.g., defining the required functionality); indeed, the committee believes that it is the involvement of such an individual in the development of the VCF that has been responsible for what success it is likely to have when it is deployed. Nevertheless, in the end there is no substitute for realism in the evolution of a prototype.

Principle 3: *In large-scale system development and deployment, testing should account for as much as 35 to 50 percent of the project schedule if a successful deployment is to be achieved.*

Testing is necessary to shake out bugs and flaws in a new system, and flaws will often be invisible until after actual users deal with actual data. The 35 to 50 percent figure above is an experience-based rule of thumb that is widely accepted among those involved with large-scale system design. Moreover, an organization without a strong track record in IT could reasonably be expected to require even more time for system testing and integration. Testing is a

[25] These comments do not mean that prototyping is a panacea that guarantees success. While prototyping usually has high value in developing requirements for user functionality, it produces results that are only as valid as the user group selected for involvement. Furthermore, obtaining realistic results from prototyping exercises requires using real-world data. Finally, prototyping is most valuable when understanding user requirements is the task at hand; it is less useful for determining reliability and response times for applications that will be deployed on a large scale.

critical dimension of system development and deployment requiring a well-developed testing strategy and a progression from unit testing to full-blown integration testing, and usually calls for dress rehearsals for system use.

The project schedule for completion of Trilogy as it was represented to the committee in October 2003 appears to leave inadequate time for testing. The committee was shown briefing charts indicating that the FBI allocated less than 10 percent of its schedule for testing, and under schedule pressure the contractor was trimming that amount even further. It was also surprising for the committee not to see, at a very late stage in VCF development, any kind of risk-based prioritization for the items remaining to be done. Instead, these items were lumped together in the category "unfixed bugs."

To provide a simple example of the need for testing, it is important to realize that the term "works" (as in the system "works") has a wide spectrum of possible meaning. Consider a simple system, consisting of a network transport layer that moves packets and is responsible for encryption and decryption and an application running on top of it. Beginning with the least demanding definition, the expression "the system works" can plausibly mean that:

1. The transport layer "lights up" but does not move application packets. Nodes can find each other, basic protocol functions such as "ping" work, and bits flow between a subset of the network and on the whole network.
2. Definition (1), and in addition data packets move between a subset of the network and on the whole network.
3. Definition (2), and in addition encryption and decryption are successful between nodes on a subset of the network and on the whole network.
4. Definition (3), and in addition the transport layer can move application packets under simulated "realistic" load between nodes on a subset of the network and on the whole network.
5. Definition (4), and in addition users in different locations can use the application to pass the appropriate information among each other.
6. Definition (5), and in addition the system functions with actual users using actual data.
7. Definition (6) with realistic numbers of users and the full complement of files.
8. Definition (7) with some reasonable assurance of the overall security of the applications, as opposed to the encrypted transport of bits alone.

In the absence of a clearly specified test plan that is acceptable to all users, it is possible to make a claim that the system "works" according to any of these definitions, even though the point of failure in the development of many systems is encountered when they are required to continue to function under load. It is unclear for Trilogy which definition of "working" is being used by those claiming that a system is working. In the case of the Trilogy infrastructure network, the VCF application is not yet available, and so it is clear that the higher levels of functionality (definition (5) and above) have not yet been attained.

2.3.2 Contracting and Contract Management

Both key contracts for Trilogy (Trilogy infrastructure and the VCF) were awarded on a cost plus/cost reimbursable basis. Only optional "tools" were awarded on a fixed-price basis. While the task orders (T0001AJM026 and T001AJM028) for both phases of the Trilogy program detail the firm fixed price to eight or nine significant figures, the task order schedules were almost totally lacking in specifications and a commitment to checkpoints. For example, the documents list a large number of plans to be created, with dates "TBD." (The committee believes that one reason underlying the lack of detail in these critical documents is that the underlying architectural work has not been done. In the absence of such architectural work, system specifications are hard to develop with any coherence.) Under these circumstances, effective program and contract management becomes essentially impossible. This weakness, aggravated by turnover among key FBI staff (e.g., the FBI chief information officer), makes it unsurprising that Trilogy is significantly behind schedule and over budget.

To illustrate some of the problems with contract management, the FBI told the committee that the Trilogy network had been made operational on March 28, 2003, only because FBI personnel in the program office were pressed into overtime service to compensate when contractors failed to meet commitments. While such efforts point to the FBI's admirable dedication to duty, the need for the program office to stand in for a contractor is a sign of contractor failure. If these "above and beyond" efforts of FBI staff could be converted into penalties for (or dismissals of) the contractors, it would send a very positive signal that the FBI program office is becoming serious about contract management.

For a contract of this magnitude and importance to the FBI and to the United States, it is imperative that senior management of the FBI monitor contractor progress closely and step in when necessary to forestall difficulties seen down the road, although day-to-day involvement is not necessary. Senior-level contract managers, experienced and empowered, should be assigned for the duration of the project, and should provide periodic actionable status information to FBI senior management. In briefings, it appeared to the committee that contractors may be viewing this project as governmental "business as usual," without due regard to the critical importance and congressional visibility of Trilogy's success or failure. Clear and detailed schedules with intermediate milestones, earned-value metrics, and severe penalties for missed delivery dates and missing functionality are desperately needed.

2.3.3 Program Management

In the committee's judgment, the FBI's program management of its IT projects is weak, and has been weak for over a year (based on the individual observations of many of the committee members who participated in the September 2002 meeting). Weak program management leads to a reactive mode in dealing with issues and a lack of overall project control. Continued cost overruns and delays often result from a lack of effective program management. By contrast, effective program management with effective management of costs and proactively managed IT projects significantly increases the likelihood of success.

For the committee, one of the most serious issues is that many essential tasks have been outsourced to vendors (e.g., development of data models and architectures). In essence, the FBI has left the task of defining and identifying its essential operational processes and its IT concept of operations to outsiders. This is not to say that outside contractors should have no role at all in these tasks, but rather that it should be the FBI, not the contractors, that defines and drives the process.

A small but telling example of the FBI's dependence on contractors is that the FBI reported no contract provisions calling for the escrow of source code for the applications. Escrow calls for the deposit of source code files and appropriate documentation with a mutually trusted third party during and after the completion of the contract. In the event that the vendor becomes unable or unwilling to continue to provide service to the FBI (e.g., the developer must be replaced because of poor performance, or the developer goes bankrupt), the source code is released to the FBI so that it can seek another vendor to assume the first vendor's responsibilities. Source code escrow is a common, even routine, commercial practice.

Program management is a well-understood discipline and set of processes. A strong program management function must be established and supported by FBI management at all levels to provide appropriate oversight and management of FBI IT projects. An effective program management function will provide the FBI with a focal point for monitoring and collecting project data and allow for the reporting of the progress of active IT projects based on well-defined metrics. (Note that program management entails a set of skills and background different from those associated with operational experience in doing investigation or intelligence analysis. That is, a single individual may have strong program management skills and extensive operational experience, and arguably a "program manager" ought to have both qualities, but there is no a priori reason to expect that someone with the former will necessarily have the latter. In any event, a program manager should at least have access to both sets of expertise.)

For program managers to be effective, they must participate deeply in the negotiation of contracts with outside vendors. The contracts must include performance measures for key deliverables, milestones, and service levels with penalties and escalation procedures. Contracts should ensure that the vendor suffers severe penalties if it is not meeting the performance measures, and major vendor failure should result in a penalty that allows the FBI to transition to a new vendor with little or no financial impact to the FBI.

Program managers are responsible for validating, monitoring, supporting, and assisting in the area of project and life-cycle costs. They may also supply information that can alter project priorities, based on resource availability or interdependent project conflicts. Most important, program managers are responsible for implementing an appropriate methodology for project management, including at least the following:

- Establishing a framework for all project communications, reporting, procedural, and contractual activity;
- Developing task-specific project plans with timelines, critical paths, and specific deliverables;
- Conducting project team meetings, setting schedules and agendas, and managing the meetings;
- Monitoring milestones and deliverables and ensuring tracking to timelines;
- Providing project status updates to key stakeholders;
- Identifying deviations from plan and addressing issues on a timely basis for resolution;
- Managing project budgets; and
- Creating an environment where the project team can succeed.

An important point is that effective program management generally requires close and frequent interactions between managers and the project team and among team members. Besides well-trained staff, the team also needs an environment that facilitates working effectively, such as proximity of offices, meeting spaces, and areas in which information can be passed informally over lunch or in a chance hallway encounter rather than relying only on formal channels of communication such as e-mail, phone calls, voice mail, teleconferencing, and meetings of high-level managers.[26]

A particularly useful management tool is a project charter. The charter includes detailed project requirements, resources, and the related roles of the project team, along with identified milestones and deliverables. Risk, issue and scope management, and communication plans are included.

The project charter is designed to do several important things. The charter should:

- Facilitate communication among stakeholders.
- Document approved purpose, scope, objectives, cost, and schedule baselines.
- Document the agreement between groups.
- Define roles and responsibilities inclusive of the overall project governance.
- Document planning assumptions and decisions.
- Provide the baseline for scope and expectation management.

In effect, the charter establishes a baseline of understanding among all stakeholders and especially between the project manager and the project sponsor(s), business owner(s), and vendor(s). The success of the project may be measured against this charter. Just as importantly, any changes must reference the charter.

2.4 ENSURING THE GROWTH OF FBI IT EXPERTISE AND DEALING WITH EXTERNAL FACTORS

The FBI recognizes, and the committee agrees, that the FBI is severely lacking in many of the technical and management skills to successfully plan, contract for, and implement a project of the breadth and scope of Trilogy. This situation must be remedied both to complete the initial phases of Trilogy, and more important, to deal with the issues described in the preceding sections. In addition to filling the top jobs such as the CIO with people who are willing to and capable of effectively managing the larger issues, a number of other gaps and constraints, some not of the FBI's making, must be addressed.

2.4.1 Human Resources

With a few exceptions, the presentations to the committee persuaded it that the FBI lacks a human resource base adequate to deal with its IT modernization program. The FBI lacks experienced IT program managers and contract managers, which has made it unable to deal aggressively or effectively with its contractors. Inexperienced managers generally lack the ability to assume proactive management roles and are often held hostage to the perspectives of the contractor.

Given the importance of IT personnel and analysts to the FBI's broadening missions, such individuals must have career track opportunities that have status and respect that are compa-

[26] Although many large organizations are able to effectively manage large-scale efforts with geographically dispersed staff, success in this regard requires a considerable degree of IT sophistication and adherence to well-defined and well-understood IT policies and practices.

rable to those of traditional personnel tracks (such as agents) within the bureau.[27] Such tracks would also enable stability in IT jobs that require extended oversight and long institutional memory.

On the positive side, the committee wishes to single out as especially noteworthy the presentations it heard from the head of security for the IT modernization program, the executive assistant director for intelligence, and the VCF project manager. These presentations reflected serious thought about their respective responsibilities from the user perspective. For example, the executive assistant director for intelligence presented a coherent and well-articulated concept of operations, as well as a clear vision of how to draw talent from the rest of the FBI. The presentations of the head of security, though not long enough to provide very much detail, were well-considered. And, the VCF project manager's operational experience has been invaluable in keeping the VCF intellectually on track.

Although the committee met only a few of them, it believes that the FBI has an important IT resource in its younger agents. The FBI agents now being hired are in their late 20's, and, as with others in their peer group, have been heavily exposed to modern forms of information technology for most of their lives. Given this fluency with information technology, it is likely that these newest agents will be the most enthusiastic about embracing new technologies to enhance their effectiveness. (Of course, the flip side is that if the organization in which they serve is unable to provide technology tools that they believe they ought to have and perceive to be adequate, they are likely to be disappointed in the organization, with all of the consequences regarding morale, work attitude, and retention.)

Finally, the committee notes that the FBI has the authority to obtain IT personnel from the private sector.[28] Under the Intergovernmental Personnel Act (IPA), the FBI can borrow personnel from other government agencies (federal, state, and local), from institutions of higher education, and from federally funded research and development centers. Generally, these arrangements call for the "home" agency or institution to pay the salary of the employee while on detail status, though the FBI could agree to reimburse the home agency as part of the terms of the cooperative agreement. IPA details cannot exceed 4 years in duration.

Under the Information Technology Exchange Program (ITEP), the FBI can enter into a *cooperative agreement* with a private sector organization for the exchange of personnel who work in the field of IT management, are considered exceptional performers, and are expected to assume increased IT management responsibilities in the future. While on detail to the FBI, the private sector organization employee may continue to receive pay and benefits from his/her employer, and the assignment may be made with or without reimbursement by the FBI for the pay, or a part thereof, during the assignment and for any contribution to the private sector organization's employee benefit systems. ITEP details cannot exceed 2 years in duration.

The FBI also has the authority to hire IT employees outright. Senior IT positions in the FBI fall under the FBI's Senior Executive Service (SES) pay scale, the range of which is $103,700 to $157,000. In exceptional cases, the FBI can pay up to $174,500, though this step requires Office of Personnel Management and Office of Management and Budget approval. The FBI is also authorized to pay a lump-sum recruitment bonus of up to 25 percent of the annual rate of basic

[27] Note that the problem of enhancing the status of workers in a critical but supporting field is common in many organizations, both inside and outside the federal government.

[28] Information on FBI hiring authorities is derived from a memo from the FBI to the committee transmitted on February 11, 2004.

pay to an employee, including individuals covered by the SES, who are newly appointed to a difficult-to-fill position.

The FBI also has available positions classified as Scientific or Professional positions that are above the GS-15 level but do not meet the SES functional criteria. These positions encompass the performance of high-level research and development in the physical, biological, medical, or engineering sciences, or a closely related field. The pay scale for such positions in the Washington, D.C., area ranges from $117,627 to $144,600.

In the judgment of the committee, these rates of pay should be sufficient to attract highly qualified IT talent. While it is true that highly qualified senior IT personnel in the private sector can command significantly higher salaries, stock options/bonuses, and the like, the FBI also offers opportunities for public service that compensate, in part, for the lower salary scales. These opportunities include the chance to have a substantial impact in service to the nation in an area of extraordinary import. The recent shift in the opportunity environment for IT people has no doubt increased the relative attractiveness of government service.

2.4.2 External Constraints

The FBI also operates under a variety of constraints that originate externally to the bureau. Two of the most significant are the following:

- *Lack of management flexibility*. Agile organizations are managerially flexible so that they can take prompt action. It is the committee's understanding that the FBI is unable to take managerial actions such as reprogramming amounts in excess of $500,000 without explicit congressional approval. This constraint and others with a similar micromanagement flavor are inconsistent with the expectation that the FBI will move quickly and forcefully to reshape itself to deal effectively with the terrorism challenge.
- *Audit pressure*. The FBI reported that it had undergone more than 100 investigations and audits in the IT area. While it is true that the FBI's performance in this area is seriously deficient (and this makes the FBI an attractive target), responding to such investigations uses the time of senior management, both in preparation and presentation of material to those investigators. And because personnel in the IT field are scarce within the FBI, the pace of work is slowed by such investigations. A better use of an equivalent amount of talent and energy would be to assist the FBI in dealing with its problems. Nevertheless, it remains the case that some audits, such as the one prepared by the General Accounting Office as *The FBI Needs an Enterprise Architecture to Guide Its Modernization Activities* of September 25, 2003 (released to the FBI August 22, 2003), contain valuable guidance.

A third area of concern is the presence of inflexible and stringent rules for personnel qualification, though the committee is not certain whether these rules originate within the FBI or outside it. Stringent rules reduce the pool from which potential employees are drawn, and inflexible rules—even undertaken in the name of upholding standards—may inappropriately disqualify otherwise qualified individuals. Of course, job applicants whose history indicates a substantial variance from the standards for employment are unacceptable. But a rule of reason ought to apply, and an otherwise-qualified applicant whose history is only minimally at variance with those standards should not be automatically excluded.

3

Recommendations

The FBI's current approach to IT modernization is not working as well as it must to support the FBI's missions in criminal investigation and preventive counterterrorism. Based on recent history, its approach is not likely to be much improved without major changes. The committee believes that a culture change within the FBI relative to IT is absolutely imperative. While the FBI needs to keep the forward thinkers among its force of experts, it will be severely handicapped unless it also culls out the elements in its leadership structure that are unable to lead the changes necessary to effectively implement an information age organization.

The first and most urgent recommendation, indeed critical in light of the impending VCF system rollout, is that the FBI not proceed with deployment of the VCF until it has a validated contingency plan for reverting completely or partially to the ACS, if necessary, and clear and measurable criteria to determine when the ACS can safely be turned off.

Beyond this urgent recommendation, the committee makes a number of recommendations, grouped into four areas, that will significantly increase the likelihood of success in and drive an accelerated pace for the FBI's IT modernization efforts. These recommendations fall into two categories. Category 1 recommendations are, in the committee's judgment, imperatives for the success of the FBI's IT modernization program, and are listed in the Executive Summary. Category 2 recommendations involve "best practices" or sound advice that the committee believes are appropriate to the FBI's situation.

3.1 REGARDING ENTERPRISE ARCHITECTURE

If the FBI is to be successful in its efforts to exploit IT, the formulation of an enterprise architecture must have the highest priority in its IT efforts. Of course, an enterprise architecture can be expected to grow and evolve to reflect the increasing responsibilities of the FBI and the increasing role that IT will have in satisfying these responsibilities, but a baseline enterprise architecture is a crucial starting point. To deal with the issues related to enterprise architecture, the committee makes the following recommendations.

Category 1 recommendations on enterprise architecture

- The committee believes that if the FBI's IT modernization program is to succeed, the FBI's top leadership, including the director, must make the creation and communication of a complete enterprise architecture a top priority. This means that they must be personally involved and invested in the key decisions that the process will require be made, such as the tradeoffs between the security of and access to information in the various data sources that are used in criminal investigation and counterterrorism efforts. Indeed, it is critical that the director be well versed in, and comfortable with, the operational aspects of the enterprise architecture and their overall linkage to the high-level system design.

Only when the FBI's leadership takes intellectual ownership of the bureau's enterprise architecture can it be used to make top-level management decisions and to ensure that IT investments realize their full potential. While a contractor might well assist the FBI in developing the enterprise architecture, no contractor will fully understand the operational issues that must be reflected in the enterprise architecture, nor be empowered to make decisions about how to make the tradeoffs with competing concerns.

The committee believes that a small team, consisting primarily of senior operational managers from the Criminal Investigation Division, the Office of Intelligence, and the Counterterrorism Division, and a senior IT executive (e.g., the CIO) to translate what these managers say into architectural terms, should be able to develop the broad outlines of the operational aspects of the enterprise architecture as well as a top-level schematic view of the systems design in a matter of 4 to 6 months of full-time work. To decide on the many operational and policy tradeoffs that will inevitably arise, this team must have direct access to and the frequent involvement of the most senior management of the FBI, including the director and the deputy director.

A reasonable first step in developing the FBI's enterprise architecture would be to define, by job, the information necessary for each FBI division to accomplish its task. The output of this effort will not be sufficient to guide implementation detail, but will provide an understanding of the information flows for investigative and intelligence data, identify existing resources, and indicate how the information needs of major categories of users can be satisfied. Further, it will provide a basis for the partitioning of implementation tasks, and identify unmet needs.

- The FBI should seek independent and regular review of its enterprise architecture as it develops by an external panel of experts with experience in both operations and technology/architecture. When the first draft of the enterprise architecture has been prepared, it should be reviewed by an external panel of independent experts charged with helping the FBI to improve how it uses IT in the long term. This could be the FBI's Science and Technology Advisory Board, an ad hoc committee or a contractor familiar with successful DOD architecture efforts, or even an ad hoc committee such as this one, but the important point is that an external inspection of the draft enterprise architecture is a sensible safeguard under any circumstances.
- Given that the counterterrorism mission requires extensive information sharing, the FBI should seek input on and comment from other intelligence agencies regarding its enterprise

architecture effort. The reason is that the FBI's information systems must have interfaces to those agencies to ensure that the information resources of those agencies are appropriately linked to FBI systems so that those agencies are able to work collaboratively.

Category 2 recommendations on enterprise architecture

- The FBI should build on the early efforts under way in the intelligence area in defining a subarchitecture for the intelligence process, rather than begin with the (implicit) architecture of the VCF. The vision for, and basic architecture of, the Trilogy system—including the VCF—predates the post-9/11 restructuring of the FBI's mission priorities and relationships to intelligence. At that time, the FBI's (and Trilogy's) focus was on support for the law enforcement mission. The change in the FBI's mission since 9/11 underscores the need for agility and for the separation of mechanism and policy in the information system architecture; many functions that would have been prohibited by policy before 9/11 are now accepted as essential parts of the FBI's operation.
- The FBI should make heavy use of scenario-based analysis in its development of an enterprise architecture. Scenario-based analysis calls for understanding relevant scenarios in sufficient detail that one can actually understand the information flows, analytic processes, and top-level decisions that must be made in those instances. Doing so will help the FBI to identify specific roles for IT in supporting operational needs.
- The FBI should give high priority to reducing the management complexity of its IT systems, even at the expense of increased costs for hardware that may appear duplicative or redundant. The successful management of a complex IT system usually requires a large degree of technical sophistication that the FBI lacks at present. As one example, the FBI should avoid the temptation to make the IDW the single repository that contains all data regardless of sensitivity or type. Section 2.2.2 points out that the access and security requirements for intelligence data and investigative data are very different, and storing both types of data on the same system will entail the implementation of a very complex set of access rules and a significant cost in human effort to maintain and enforce those rules. The cost of the extra complexity entailed by the single-repository concept will, in the long run, far outweigh the cost of the "extra" hardware.

Box 1 provides a sampling (not an exhaustive or complete list) of some of the elements that the committee would expect to see in the FBI's enterprise architecture.

3.2 REGARDING SYSTEM DESIGN

To deal with the most important of the system issues described in Section 2.2, the committee makes the following recommendations:

Category 1 recommendations on system design

- The FBI should refrain from initiating, developing, or deploying any IT application other than the VCF until a complete enterprise architecture is in place. The committee hopes that the initial operating capability of the VCF will soon be demonstrated. If successful, it will

BOX 1: A Sampling of Items That Should Be Present in the Enterprise Architecture

An enterprise architecture is generally represented as a set of operational diagrams accompanied by appropriate narratives that show the operating elements or nodes constituting the enterprise, the data/information flow requirements between the nodes, and other data reflective of the operational structure. It is the central document describing the operational, system, and technical views of the enterprise. Central to an enterprise architecture is a clear description of key processes and how they can be supported and enhanced by appropriate application of technology. The enterprise architecture specifies the overall design and the set of building codes to which deployed systems must conform in order to make the IT investment effective.

The following listing is a sampling (not complete in any way) of items that the committee would expect to see in the FBI's enterprise architecture.

a. All significant information inputs are shown, with identification of sources and restrictions on their use, if any.
b. Processes that are primarily investigative and those that are primarily counterterrorism- or intelligence-specific are identified. Some processes and flows may be in both domains.
c. Some supportive operational processes interact with the investigative and counterterrorism processes and are labeled as being in the support business category.
d. The VCF is shown as one of a number of information sources that feed the intelligence process.
e. The VCF is shown as the primary source of information for the investigative process.
f. Different subarchitectures are reflected for each major operational process found in the FBI (e.g., for the intelligence and investigative processes). The VCF system is seen to span investigative processes, but does not play a primary role in implementing analytic processes.
g. Interfaces between subarchitectures are defined and specify the data flows between them (e.g., the relationship between the records management process and the intelligence and investigative processes). Standards for data exchange are explicitly acknowledged.
h. Responsibility for the contents of all persistent storage systems or their segments (e.g., data cleansing and validation) are assigned, documented, and represented.
i. Data access constraints, such as law-enforcement-sensitive data and levels of classified and open data, are explicitly identified. Different approaches to security (e.g., risk management versus risk avoidance) are articulated explicitly and provide the framework that allows management to make decisions about tradeoffs.
j. Data storage applications are logically disjoint whenever they have different governing policies (or else a credible argument for doing otherwise is demonstrated).
k. The relationship between the VCF and records management systems is explicitly represented, and responsibilities for maintaining evidence for investigations are highlighted.
l. Data models for the different processes are specified. Any significant differences in data models that need to be unified to serve both the investigative and analytic functions are represented.
m. Access requirements for data supporting the various processes are clearly specified, including any audit trail requirements.
n. Release constraints for data and results emanating from the various processes are clearly specified, including any audit trail requirements.
o. Policies for replication of information among data storage applications are specified.
p. The use of an electronic key management system developed by the National Security Agency in the context of the specific needs of the FBI is explicitly rationalized.
q. Process and data interfaces with other law enforcement organizations (international, state local, and tribal) are identified.
r. Specific databases and controlled interfaces between them (if any) are identified.
s. A map between these interfaces and the physical network configuration shows what links/nodes must be encrypted, physically protected, or both.
t. A key-management plan (for managing encryption keys) is created.
u. A vulnerability assessment (i.e., a paper attack on the paper architecture) is conducted.

provide such a major step forward from the ACS that it would be a mistake to halt VCF development and deployment at this time. But in the committee's view, the benefit of designing future applications within the enterprise architecture framework is so large, and the risk of designing without that framework in place so high, that no additional development should proceed until the framework is in place.[1]

- The FBI should develop a process map for information sharing that clearly defines the current state of and a desired end state for the information-sharing process so that the numerous information-sharing initiatives can be coordinated and properly monitored and managed. This recommendation is derived from the DOJ inspector general report[2] but is one that the committee fully supports. In a letter to the DOJ inspector general dated December 11, 2003, the FBI stated that it had already completed a detailed blueprint and process map on its intelligence and information sharing process,[3] but as of December 2003, neither the committee nor the DOJ inspector general had been able to review this document.[4]
- The FBI should immediately develop plans that address recovery of data and functionality in the event that essential technology services come under denial-of-service attacks (e.g., from viruses and pervasively replicated software bugs). In addition, the FBI should deploy technically distinct platforms (that is, computing nodes that are based on a different operating system) for the hosting or backup of critical services or data, so that in the event of a global attack on the Trilogy network, these services are more likely to be maintained and the uninfected platforms can serve as a "beachhead" from which cleanup operations can be mounted.

Category 2 recommendations on system design

- The FBI should develop a future release plan for the VCF that specifies what capabilities will be added to it, and in what order and time frame. The committee believes that future releases of the VCF, other than those needed to reach initial functionality, should be delayed until an overall enterprise architecture is in place. Further, the FBI should ensure that the first enhancements to the VCF are to make the system consistent with the overall enterprise architecture (rather than only to add additional functionality). After that, capabilities to be considered include the addition of a separate workflow engine (a high priority, as described below) and the creation and integration of interfaces to the IDW. Developing the plan in the context of the enterprise architecture is critical to aligning the development activities of the IDW, SCOPE, and the VCF, and other systems and to optimizing what will likely be significant investments downstream.
- The FBI should plan to rework the next version of the VCF to include a workflow engine as a high priority. By incorporating a workflow engine, the FBI will make the VCF more agile

[1] The GAO position, as documented in the GAO commentary on the FBI response, is that it is acceptable for the FBI to be "pursuing near-term IT upgrades before it completes and is positioned to use an architecture," even though pursuing these upgrades "without a blueprint that provides an authoritative, commonly understood frame of reference that translates strategy into implemental actions . . . [will increase] modernization risk." (Response of the FBI to the GAO report *The FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*, dated September 22, 2003. Available at http://www.gao.gov/new.items/d04190r.pdf.) The committee concurs with the GAO position only for the VCF application and believes that for all other applications, the risk of proceeding without an enterprise architecture in hand is too high.

[2] DOJ report available at http://www.usdoj.gov/oig/audit/FBI/0410/app8.htm.

[3] FBI letter available at http://www.usdoj.gov/oig/audit/FBI/0410/app7.htm.

[4] See http://www.usdoj.gov/oig/audit/FBI/0410/app8.htm.

in its support of evolving FBI policies and practices, reduce the expense of evolving the VCF application, reduce the risk of delaying implementation of new policies and practices, and extend the lifetime of the VCF application. (Note that commercial workflow engines are available that can be configured to support a myriad of workflow arrangements without modifying the application programs they serve. Workflow engines are a common technology that is employed by many organizations, especially those that are large, complex, and geographically dispersed. Furthermore, IT staff might well include specialists trained in human computer interaction who can understand process flows and how to build systems that reflect new protocols of agents and analysts.)

- The FBI should adopt a risk management approach to security, for only in doing so will it understand the operational penalties it pays for risk avoidance. Acceptance of this premise results in several immediate items of high priority.

  —The FBI should establish a clear policy governing sensitive but unclassified (SBU) and law-enforcement-sensitive communications (and data more generally). Such a policy can be risk-based.

  —The FBI should reconsider, in the light of a better understanding of the risk/benefit tradeoffs to its missions, the very constrained access that FBI staff have to the Internet.

  —The FBI has stated that it is in the process of acquiring a risk management tool that will assist it in determining where IT vulnerabilities should be mitigated through risk/cost trade-offs, thereby ensuring IT continuity of operations, and that this tool will be interfaced with tools that the FBI uses to develop and manage its enterprise architecture efforts. These efforts should continue, although the committee notes that the threat driving the need to ensure continuity of operations in the face of attack differs in kind from the threat of compromising sensitive information.

  If the FBI is not comfortable with moving to a risk management approach to security, at the very least it should review security practices in a risk-versus-reward framework with an entire end-to-end consideration of the information gathering and information management requirements of the FBI's staff.

- The FBI should encourage creative experimentation with exploitation of IT in the field, such as the PDA experiment mentioned in Section 2.2.4 above. The committee did not review this area in detail, but it believes that such experimentation, with appropriate safeguards, has enormous potential for helping the FBI to understand how its operational processes might be improved through the use of IT. Further, the learning from these efforts to anticipate the technological future should be brought forward and become an important input into the bureau's strategic planning process in order to accelerate its pace of modernization. (In this regard, a useful philosophy is the one underlying the Department of Defense's Advanced Concept Technology Demonstration programs, which are based on an integrating effort, undertaken by an ultimate user, to assemble and demonstrate a significant new military capability in a realistic environment, based on maturing advanced technologies, to clearly establish the capability's military utility.[5])

[5] For more information, see http://www.acq.osd.mil/asc/.

3.3 REGARDING PROGRAM AND CONTRACT MANAGEMENT

To deal with the most important of the program management issues described in Section 2.3, the committee makes the following recommendations.

Category 1 recommendations on program management

- Because testing is such a critical dimension of system development and deployment, the FBI must allow adequate time for testing before any IT application (including the VCF) is deployed, even if dates of initial operational capability are delayed. Testing must include a full systems integration test and adequate scale, volume, and stress tests.
- Evolution is an essential component of any large system's life cycle. Future development contracts for user applications should be premised on the use of small-scale prototypes that can be built rapidly and tested with user feedback before committing to large-scale development. Therefore, in future IT applications development, particularly of large-scale end-user-oriented applications, procurement contracts should be conditioned on the development of small-scale prototypes that can be built rapidly and tested with user feedback before committing to large-scale development.
- For IT applications beyond the VCF, the FBI should exploit proven methodologies of contracting and contract management, including the use of detailed functional specifications, specific milestones, frequent contract reviews, and earned-value metrics. Given the FBI's problems with the management of the Trilogy program, the next contract review should focus on continuity and availability. Contracts already in place should be renegotiated to include best practices such as code escrow and support-service-level agreements to protect the FBI against operational failures that can adversely impact the availability of and support for products that the FBI will depend on. The FBI should consult with both other government agencies and the private sector to develop a set of best contracting practices before undertaking its next contract review.

Category 2 recommendations on program management

- The FBI's contracting strategy should be tied to features of its enterprise architecture; e.g., it should identify opportunities for multiple, smaller contracts with well-defined deliverables and major progress checkpoints. This strategy should also highlight areas in which the FBI requires in-house or trusted technical expertise to define and manage key concepts that govern contracts and relationships between contractors. (This kind of information derives from the architectural triad described in Section 2.1.1. For example, the system architecture should define the major systems to be built. The technical architecture should define the key interfaces between systems that have to be carefully managed to get independently developed component systems to work together. In addition, the FBI should have in-house expertise regarding operations as they relate to the overall infrastructure, whereas the FBI may be able to leave to contractors the expertise relevant to functionality in specific instances and specific applications.

3.4 REGARDING HUMAN RESOURCES

To deal with the most important of the skills issues described in Section 2.4, the committee makes the following recommendations.

Category 1 recommendations on human resources

- For Trilogy and subsequent IT projects to have access to the human talent they need to succeed, the FBI must dramatically grow its own internal expertise in IT and IT contract management as quickly as possible. To deal with human resource shortages in key areas (e.g., program management, data architecture, data modeling, and data warehousing), the only feasible short-term fixes are to borrow experienced personnel from other agencies or to obtain assistance through a memorandum of understanding or agreement (MOU/MOA) from another government agency with substantial experience in the relevant matters. The expectation would be that these arrangements would last for a couple of years, during which time the FBI could train permanent replacements in long-term career tracks with the FBI.

Note that this recommendation is still consistent with the notion of using outside expertise, when it is appropriate, as long as the FBI does not cede overall management and the making of the key decisions. For example, the FBI could in principle outsource in a secure facility the day-to-day operation of its information systems and thus conserve its scarce IT talent to work on matters more closely related to operations and strategy.

- Because of their importance to the short- and long-term success of the bureau's IT modernization efforts, the FBI must permanently fill the positions of chief information officer and chief enterprise architect, and the committee concurs with the director's judgment that filling these positions with appropriately qualified individuals ought to have the highest priority. At this writing (late March 2004), an acting CIO and an acting chief technology officer have been appointed. The appointment of these individuals is promising, and unverified reports suggest that they are committed to completing the enterprise architecture in a matter of months, although the committee underscores once again the need for the operational management to be heavily involved in the creation of the enterprise architecture.
- The FBI should develop an improved system for internally reviewing the state of progress in key IT programs and for communicating relevant findings to key stakeholders, thus preempting the perceived need for and distraction of constant external investigations.

Category 2 recommendations on human resources

- The FBI should seek relief from excessively tight constraints on reprogramming allocated funds, or at least seek to streamline the approval process.

3.5 CONCLUSION

The committee believes that the FBI has made significant progress in some areas of its IT modernization efforts, such as the modernization of the computing hardware and baseline software and the deployment of its networking infrastructure. However, because the FBI IT infrastructure was so inadequate in the past, there is still an enormous gap between the FBI's current IT capabilities and the capabilities that are urgently needed.

The committee has made recommendations that, if adopted, will significantly increase the likelihood that the FBI's Trilogy IT modernization program will enhance the FBI's effectiveness in carrying out its critical crime-fighting and counterterrorism missions. But it emphasizes the difference between a pro forma adoption of these recommendations and an adoption of these recommendations that is both fully embraced throughout the agency and aggressively executed. The former may be the metric that auditing and oversight agencies and offices often use in assessing agency performance, but it is the attitude and willingness of senior staff to act that really count. The senior management of the FBI has a substantive and direct role to play in the FBI's IT modernization efforts. This role either has not been understood or it has been given a lower priority based on the perception of more immediate operational priorities. Given the importance of IT to the FBI's future success in carrying out its missions, the FBI's senior management must concern itself as much with developing a coherent vision for using IT to advance the bureau's strategic view as with budgets, training programs, equipment, and organization. As the complexities of the FBI's evolving role are understood, the committee believes that investment by the FBI's senior management team in the IT process will yield major enhancements to mission achievement as well as substantial operational efficiencies.

Appendix

Short Biographies

James C. McGroddy, *Chair,* retired from IBM as a senior vice president, research at the end of 1996, after leading its research laboratories from 1989 to 1995. During his tenure, which spanned the period of IBM's most difficult challenges, he led a major restructuring of its research efforts, building a model and management system that is now widely emulated. One of the measures of success was the creation during this period of two new laboratories, one in Beijing and one in Austin, Texas. His leadership was recognized by his being awarded the Frederik Philips Medal of the Institute of Electrical and Electronics Engineers and the George Pake Award of the American Physical Society. He is currently an advisor to several government agencies, is a participant in a number of National Research Council groups, and serves as an advisor and a visitor at a number of universities in the United States and Europe. McGroddy is the chairman of the board of MIQS, a company providing clinical information systems and electronic medical record capability aimed at improving the quality and cost-effectiveness of the care of the chronically ill. As chairman of the board of the Stellaris Healthcare Network in 2000 and 2001 and as former chairman of the board of Phelps Memorial Hospital Center, he has been heavily involved in the restructuring of the local health care delivery system in Westchester County. He is a director of Paxar, Inc., and of Advanced Networks and Services, Inc. He is also a trustee of his alma mater, St. Joseph's University in Philadelphia, as well as a member of the advisory boards of a number of start-up firms and university departments. McGroddy originally joined IBM in its Research Division in 1965 after receiving a PhD in physics from the University of Maryland. He earned his BS in physics from St. Joseph's University in Philadelphia in 1958. In his first years at IBM, he focused on research in solid state physics and electronic devices, and as a result of achievements in these areas was named a fellow of both the IEEE and the American Physical Society. In the 1970-1971 academic year, he was a visiting professor of physics at the Danish Technical University. Returning to IBM, he served in a number of management positions in research, development, and manufacturing before being named IBM's director of research in 1989. He is a member of the U.S. National

Academy of Engineering. McGroddy chaired the CSTB committee that produced the report *Realizing the Potential of C4I: Fundamental Challenges*.

Ed Balkovich is a senior engineer at RAND. His current research focuses on telecommunications and information technologies, and infrastructure. Prior to joining RAND, he was a director in the technology organization of Verizon Communications (formerly Bell Atlantic). While at Verizon, he led technology assessment activities focused on the use of IP networks in telecommunications. His work included the design and deployment of Verizon's first voice services for IP networks, and prototypes of video, voice, and VPN concepts delivered by DSL access and IP networks. In addition to technology assessment, he also played a significant role in understanding and explaining the policy implications of emerging technologies and IP networks. His policy contributions concerned both regulatory and law enforcement issues. While at Verizon, he served on the CSTB committee that produced *Realizing the Potential of C4I: Fundamental Challenges*, and a follow-up workshop convened to explore a security recommendation made in the committee's report. Before joining Verizon, he was a member of Digital Equipment Corporation's Cambridge Research Lab. While at Digital he was the first associate director of MIT's Project Athena (which developed X-windows, Kerberos authentication, and Zepher messaging). He contributed to various engineering and research projects, as well as customer applications spanning the areas of clustered computing, telecommunications, virtual private networks, and electronic publishing. His work with customer applications helped to define and create an internal consulting organization supporting leading-edge applications of computing and networks by customers. He worked in the aerospace industry prior to joining Digital. In addition to his industrial experience, he has held research and academic appointments at MIT, Brandeis, the University of Connecticut, and the University of California. He holds doctorate and master's degrees in electrical engineering from the University of California, Santa Barbara, and a bachelor's degree in mathematics from the University of California, Berkeley.

Richard J. Baseil was most recently with the MITRE Corporation, managing MITRE's systems engineering of IT for the U.S. Army. He was also with Cisco Systems, working on voice services over data communications networks. Previously, he was vice president in Telcordia Technologies' Professional Services organization. Mr. Baseil has managed product testing and quality analyses of telecommunications switching, signaling, transport, and customer-premise systems, with an emphasis on hardware and software interoperability. He also advises telecommunications service providers on improvements to their procurement processes for network systems. Mr. Baseil played a major role in defining the industry need for, and subsequently establishing, a multi-company Internet work interoperability test planning effort in the United States, and he managed the Telcordia staff and the interconnection facility used by industry participants to conduct nationwide signaling and interoperability testing. Mr. Baseil has 30 years of IT and telecommunications experience, having had responsibility for switching systems engineering, signaling network engineering, operations systems engineering, operating services system requirements, network database requirements, ISDN data services engineering, billing services, and some early descriptive work on next-generation switching systems. Mr. Baseil holds bachelor's and master's degrees in electrical engineering from the New Jersey Institute of Technology. He served on the CSTB committee that produced *Realizing the Potential of C4I: Fundamental Challenges*.

Matt Blaze, a professor at the University of Pennsylvania, studies the use of cryptography in computing and network security. His research focuses on the architecture and design of secure systems based on cryptographic techniques, analysis of secure systems against practical attack models, and finding new cryptographic primitives and techniques. He is the co-inventor of the field of trust management, and he headed the KeyNote project at AT&T Laboratories. His recent work and collaborations have led to the creation of new cryptographic concepts, including remotely keyed encryption, atomic proxy cryptography, and master-key cryptography. His research has also been influential in IP network-layer, session-layer, and file-system encryption. Blaze has discovered weaknesses in a number of published and fielded security systems, including a protocol failure in the U.S. Clipper key-escrow system. Blaze has long been active in the debate on encryption and security policy, has testified before Congress several times, has participated in influential public-policy panels and reports, and created the Web resource crypto.com. He holds a PhD in computer science from Princeton University.

W. Earl Boebert is an expert on information security, with experience in national security and intelligence as well as commercial applications and needs. He is a senior scientist at Sandia National Laboratories. He has 30 years of experience in communications and computer security, is the holder or co-holder of 13 patents, and has participated in CSTB studies on security matters. Prior to joining Sandia, he was the technical founder and chief scientist of Secure Computing Corporation, where he developed the Sidewinder security server, a system that currently protects several thousand sites. Before that he worked for 22 years at Honeywell, rising to the position of senior research fellow. At Honeywell he worked on secure systems, cryptographic devices, flight software, and a variety of real-time simulation and control systems, and he won Honeywell's highest award for technical achievement for his part in developing a very large scale radar landmass simulator. He also developed and presented a course on systems engineering and project management that was eventually given to more than 3,000 students in 13 countries. He served on the CSTB committees that produced *Computers at Risk: Safe Computing in the Information Age, For the Record: Protecting Electronic Health Information*, and *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*. He also participated in two of CSTB's workshops, "Cyber-Attack" and "Insider Threat."

Marc Donner is an executive director in the Institutional Securities Division of Morgan Stanley, where he focuses on system and data architecture around client relationships. His recent projects have included initiating Morgan Stanley's Internet presence and intranet activities and modernizing a number of legacy systems. He received a bachelor's degree in electrical engineering from the California Institute of Technology and a doctorate in computer science from Carnegie Mellon University. He is a member of the IEEE Computer Society and Usenix.

Michael McGill has more than 30 years of hands-on experience in information technology and more than 12 years in health care technology. He has been responsible for systemwide operations and for the development of information systems. He has also been responsible for the development of clinical data repositories, overseen the implementation of clinical and administrative systems, and developed support architectures that allow secure and reliable access. Dr. McGill was the corporate vice president and chief information officer of the Henry Ford Health System, an integrated health care delivery system. Prior to that he was the chief information officer of the University of Michigan Health System. At the University of Michigan, McGill also headed its telecommunication networks and phone service. He led the evolution of the electronic information resources at both the University of Michigan and Henry Ford. Dr. McGill served as a director of industry marketing with Ameritech Information Systems. He was vice president of Online Computer Library Center, Inc. At Syracuse University, he held the positions of associate professor, assistant dean for research and the PhD program, School of Information Studies, and associate professor in the School of Computer and Information Science. He was program director for information science for the National Science Foundation and a senior computer and information science advisor, Office of Toxic Substances, U.S. Environmental Protection Agency. He holds a bachelor's degree from Michigan State University and master's and doctoral degrees in computer science from Syracuse University. Dr. McGill is a member of the American Medical Informatics Association, the College of Health Information Management Executives, and the Health Information Management Systems Society. He has been elected a fellow of the American Association for the Advancement of Science for his "pioneering research and development in information systems." He is also the author of numerous articles and co-author of *Introduction to Modern Information Retrieval*, published by McGraw-Hill.

James Noga is the CIO for the Massachusetts General Hospital. The 875-bed hospital with over 1.4 million ambulatory visits annually is a world-renowned medical center offering sophisticated diagnostic and therapeutic care, and it conducts the largest hospital-based research program in the United States. He came to the MGH in 1990 as director of clinical applications and in 1997 became the CIO. He has been instrumental in advancing clinical systems at the MGH with the introduction of an online enterprise clinical reporting system, provider order entry, and an ambulatory electronic medical record. In addition to clinical systems his current focus is on improving patient revenue cycle systems. He is also a contributor to the recently published book *Effective Healthcare Information Management: Leadership Roles, Challenges, and Solutions* on the topics of software procurement and integration strategies. Mr. Noga holds an MS degree in biomedical computing and information processing from the Ohio State University and is an active member of the College of Healthcare Information Management Executives and Society of Information Management.

Carl G. O'Berry is vice president, Strategic Architecture, Integrated Defense Systems, The Boeing Company. He was previously deputy chief of staff for Command, Control, Communications & Computers, Headquarters, U.S. Air Force, a position from which he directed Air Force-wide information systems planning and policy development. Earlier in his Air Force career, he served as commander of the Air Force Rome Air Development Center and as joint program manager, World-Wide Military Command and Control System Information System. He also led the development and field testing of an airborne radar sensing/tracking system that was the forerunner of the Joint Surveillance and Target Attack Radar System. He has a master's degree in systems management from the Air Force Institute of Technology and a bachelor's degree in electrical engineering from New Mexico State University. He served on the CSTB committee that produced *Realizing the Potential of C4I: Fundamental Challenges*. He retired from the U.S. Air Force as a lieutenant general in August 1995. From then until December 1998, he was vice president and director of planning and information technology for Motorola, the Space and Systems Technology Group, in Scottsdale, Arizona.

Ken Orr is an internationally recognized expert on data warehousing, knowledge management, software engineering, business process reengineering, and technology transfer. He is the founder and principal researcher of the Ken Orr Institute, a business technology research organization. Previously, Mr. Orr was an affiliate professor and director of the Center for the Innovative Application of Technology with the School of Technology and Information Management at Washington University in St. Louis. Mr. Orr has more than 39 years of experience in research, analysis, design, project management, technology planning, and management consulting. His clients have included such organizations as the states of California, Illinois, Kansas, Michigan, Minnesota, Missouri, Oregon, and Washington, the city of Chicago, the U.S. Army, Navy, and Marine Corps, the FAA, IBM, DEC, Detroit Edison, Xerox, Olivetti (Italy), Philip Morris, Pacific Bell (SBC), Bellcore (Telcordia), Burlington-Santa Fe Railroad, Kellwood Corporation, Phoenix International (Canada), and many others. Mr. Orr has written three books (*Structured Systems Development*, *Structured Requirements Definition*, and *The One Minute Methodology*) and is the author of dozens of articles on advanced software development, technology management, and human communication. Mr. Orr was also one of the principal developers of the DSSD (Warnier-Orr) methodology, as well as a leading researcher in the development of automated tools for automatic program generation, database design, business requirements, and advanced client/server prototyping.

James Patton is a technical director with the MITRE Corporation, currently helping lead an organization of over 200 persons devoted to numerous information systems challenges of the extended intelligence and law enforcement communities. He has nearly 30 years of information systems experience, with over 20 of those years focused on the peculiar needs and challenges of distributed systems for intelligence support. Mr. Patton has done performance engineering, including synthetic workload modeling and benchmarking, as well as providing and managing the provision of systems engineering expertise for the acquisition of large-scale distributed systems through all phases of the systems engineering process. He has managed work programs seeking to apply current and near-term information technologies in innovative ways to address challenging intelligence problems. Mr. Patton received a bachelor's degree in mathematics from Loyola College and did graduate study in applied mathematics and computer science at Rice University.

Mark Seiden is a senior consultant with Cutter's Business-IT Strategies Practice and a member of the Leadership Group of Cutter Consortium's Risk Management Intelligence Network. He has consulted since 1983 in the areas of security, network, and software engineering to companies worldwide, with clients including start-ups, major computer and communication companies, financial institutions, law firms, UN agencies, online content providers, Internet service providers, research organizations, and nonprofits. As an independent consultant, and in varying roles at Securify (also known as Kroll O'Gara Information Security Group), his most recent projects have included design, architecture, and implementation for e-business systems; security for online financial transaction processing and distributed document processing systems; custom firewalls based on open-source components; finding computer criminals; and penetration testing of the network and physical security of deployed systems, enterprises, and colocation facilities. Mr. Seiden has 35 years of programming experience. He has been a Unix and mainframe system programmer; written Macintosh applications; spent time at IBM Research, Xerox Parc, Bell Labs, and Bellcore; and has taught at the university level. Mr. Seiden has been on the board of directors of two user groups and is on the Technical Advisory Board of Counterpane Security Systems.

George Spix is chief architect in the Consumer Platforms Division of Microsoft Corporation. He is responsible for Microsoft's end-to-end solutions for consumer appliances and public networks. He also serves on the board of the Digital Audio Video Council, the Information Infrastructure Standards Panel, the Commerce Department's Computer Systems' Security and Privacy Advisory Board, and a National Research Council study focused on trusted computing systems. Mr. Spix joined Microsoft in 1993 as the director of multimedia document architecture. He was responsible for the Advanced Consumer Technology Division's multimedia tools efforts and early third-party tools acquisitions. Later, as director of infrastructure and services, he led a team that created the services and networks required for early interactive television trials. Before coming to Microsoft, Mr. Spix spent 5 years as director of systems and software development at Supercomputer Systems, Inc., in Eau Claire, Wisconsin. He was responsible for the delivery of systems and software products for a next-generation supercomputer. Prior to that, he worked for Cray Research, Inc., in Chippewa Falls, Wisconsin, as a chief engineer and was responsible for systems and software development for the XMP and YMP line of supercomputers. A Purdue University electrical engineer, Mr. Spix was drawn to supercomputers, their systems, and applications while at the Los Alamos National Laboratories.

Charles E. Stuart is president and CEO of Competitive Enterprise Solutions, LLC (CESLLC), a networking and information technology consulting firm he founded in 1999. At CESLLC he has contributed to projects addressing computer security, machine learning, and enterprise collaboration. In the past year he has been supporting the development of a next-generation intrusion detection system with sponsorship from DARPA and Rome Laboratories and is currently working with a client to commercialize that technology. Prior to founding CESLLC, Mr. Stuart spent 20 years in government service. As a senior executive in the Department of Energy's Nuclear Weapons Program, Mr. Stuart was responsible for implementing enterprise collaboration tools for streamlining and improving design and manufacturing processes at the plants and national laboratories. These included Web-based tools for resource planning as well as for design modeling and simulation. In addition, for 2 years he was a manager in the Advanced Simulation and Computing Initiative, which produced the first teraop computing platform, and in 1998 he led a study of networking security requirements for the weapons complex. During the Cold War, prior to his DOE service, Mr. Stuart spent 25 years as both a contractor and civil servant in the field of undersea warfare. He founded and headed the Maritime Systems Technology Office at DARPA, where he served as both a program manager and office director. In 1985 he received the Bushnell Award from the American Defense Preparedness Association for his career contributions to undersea warfare. Mr. Stuart holds a BSEE degree from Duke University and completed a 2-year program in business and management. His biography is included in *Who's Who in America* and *Who's Who in Science and Engineering*. He is a member of the IEEE and the National Defense Industrial Association.

Gio Wiederhold is a professor (emeritus) of computer science, medicine, and electrical engineering at Stanford University. He started working with computers for numerical applications in 1957. In the late 1960s he led the development of real-time data acquisition and database systems to support clinical research. Derivative products from that work are still being used at Stanford and around the world. After gaining 16 years of industrial experience, he returned to school and joined the Stanford faculty in 1976. At Stanford he initiated research into knowledge-based techniques for information and database management. This research direction, starting with the KBMS project at Stanford in 1977, has now become an active research field in its own right. Results derived from this work help in the management of complex information systems, as found in medicine, especially long-term-care records, manufacturing systems, and planning applications. His current focus has shifted to the problems encountered in the integration and composition of large-scale networked and software systems. He holds a PhD in medical information science from the University of California, San Francisco, and a degree in aeronautical engineering from TMS Technicum in Rotterdam, Holland. Dr. Wiederhold has been a fellow of the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers. He has participated with the Air Force Scientific Advisory Board and has served on numerous National Research Council committees. He has also been a DARPA program manager.

Staff Members

Herbert S. Lin is senior scientist and senior staff officer at the Computer Science and Telecommunications Board, National Research Council of the National Academies, where he has been the study director of major projects on public policy and information technology. These studies include a 1996 study on national cryptography policy (*Cryptography's Role in Securing the Information Society*), a 1991 study on the future of computer science (*Computing the Future*), a 1999 study of Defense Department systems for command, control, communications, computing, and intelligence (*Realizing the Potential of C4I: Fundamental Challenges*), and a 2000 study on workforce issues in high-technology (*Building a Workforce for the Information Economy*). Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He also has significant expertise in math and science education. He received his PhD in physics from MIT in 1979. Avocationally, he is a longtime folk and swing dancer, and a poor magician. Apart from his CSTB work, a list of publications in cognitive science, science education, biophysics, and arms control and defense policy is available on request.

Kristen Batch is a research associate with the Computer Science and Telecommunications Board of the National Research Council. She will be involved with upcoming projects focusing on wireless communication technologies and telecommunications research and development. While pursuing an MA in international communications from American University, she interned at the National Telecommunications and Information Administration, in the Office of International Affairs, and at the Center for Strategic and International Studies, in the Technology and Public Policy Program. She also earned a BA from Carnegie Mellon University in literary and cultural studies and Spanish, and received two travel grants to conduct independent research in Spain.

What Is CSTB?

As a part of the National Research Council, the Computer Science and Telecommunications Board (CSTB) was established in 1986 to provide independent advice to the federal government on technical and public policy issues relating to computing and communications. Composed of leaders from industry and academia, CSTB conducts studies of critical national issues and makes recommendations to government, industry, and academic researchers. CSTB also provides a neutral meeting ground for consideration of complex issues where resolution and action may be premature. It convenes invitational discussions that bring together principals from the public and private sectors, ensuring consideration of all perspectives. The majority of CSTB's work is requested by federal agencies and Congress, consistent with its National Academies context.

A pioneer in framing and analyzing Internet policy issues, CSTB is unique in its comprehensive scope and effective, interdisciplinary appraisal of technical, economic, social, and policy issues. Beginning with early work in computer and communications security, cyber-assurance and information systems trustworthiness have been a cross-cutting theme in CSTB's work. CSTB has produced several reports regarded as classics in the field, and it continues to address these topics as they grow in importance.

To do its work, CSTB draws on some of the best minds in the country, inviting experts to participate in its projects as a public service. Studies are conducted by balanced committees without direct financial interests in the topics they are addressing. Those committees meet, confer electronically, and build analyses through their deliberations. Additional expertise from around the country is tapped in a rigorous process of review and critique, further enhancing the quality of CSTB reports. By engaging groups of principals, CSTB obtains the facts and insights critical to assessing key issues.

The mission of CSTB is to:

- ***Respond to requests*** from the government, nonprofit organizations, and private industry for advice on computer and telecommunications issues and from the government for advice on computer and telecommunications systems planning, utilization, and modernization;
- ***Monitor and promote the health of the fields*** of computer science and telecommunications, with attention to issues of human resources, information infrastructure, and societal impacts;
- ***Initiate and conduct studies*** involving computer science, computer technology, and telecommunications as critical resources; and
- ***Foster interaction*** among the disciplines underlying computing and telecommunications technologies and other fields, at large and within the National Academies.

More information about CSTB can be obtained online at http://www.cstb.org.