NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

1100 New York Ave NW, Ste 1090 East
Washington, D.C. 20005

TEL (202) 347-3190 FAX (202) 393-0993
INTERNET: www.napawash.org

Dick Thornburgh

Chairman

Academy Panel on FBI Reorganization

Testimony

Before the

**Subcommittee on Commerce,
State, Justice, the Judiciary, and Related Agencies
Committee on Appropriations
House of Representatives**

June 18, 2003

Chairman Wolf, Representative Serrano, and Members of the Subcommittee.

I appreciate the opportunity to appear before the Subcommittee to discuss the Federal Bureau of Investigation's (FBI's) reorganization. I am speaking today as Chair of the National Academy of Public Administration's Panel on the FBI Reorganization. The Academy is an independent non-profit organization chartered by Congress to assist public institutions in improving their performance. Other members of the Academy's Panel include Robert Alloway, Frank Chellino, Martin Faga, Kristine Marcy, Robert O'Neill, and Harold Saunders. (See Attachment A)

In June 2002, on behalf of the Academy's Panel, I testified before this Subcommittee on the FBI's proposed reorganization plan. Specifically, we:

- endorsed the creation of the five new divisions Director Mueller recommended
- suggested additional steps to help implement the reorganization successfully
- expressed concerns about information technology and information sharing, that were critical to combating terrorism and improving the FBI's overall performance

This Subcommittee subsequently approved that plan.

The urgency of Congressional action last year required the Panel to expedite its review. However, at the Subcommittee's request, we have continued to monitor and assess the FBI's reorganization progress this year in seven key areas. These are the five new divisions created by the reorganization, plus information technology and drug enforcement.

During this review, we have received complete cooperation from Director Mueller and other FBI and Justice officials. Despite the hectic pace of events, they have been generous with their time and responsive to requests for information. Also, I would like to express our appreciation to General Accounting Office (GAO) and its staff. They have monitored progress in other key areas related to the reorganization, such as strategic planning, personnel recruitment and training, and internal controls. Our respective staffs coordinated their efforts and shared information and insights to avoid unduly burdening the FBI. Finally, I am pleased to note that, since 9/11, Congress has not added to an already long list of federal crimes within the FBI's jurisdiction. This is commendable and enables the FBI to devote increased attention and resources to counterterrorism.

Mr. Chairman, at the outset, it is important to recognize that the FBI reorganization is being carried out at a time when governmental strategies, policies, programs, and organizations are in tremendous flux. New strategies on national security, homeland security, cyberspace, and on combating terrorism and weapons of mass destruction were promulgated during the last year. These have been accompanied by major organizational changes. Shortly after the FBI requested Congressional approval of its reorganization, the President asked Congress to create a new Department of Homeland Security (DHS). It was established on March 1, 2003. Also, in his February 2003 State of the Union address, the President announced the consolidation of FBI, DoD, DHS, and intelligence community elements in a new Terrorist Threat Integration Center (TTIC). It began operations in early May. Finally, increased counterterrorism activities and new programs associated with wartime operations were directed in the post-9/11 Emergency Supplemental and in the Iraqi supplemental.

In addition, these changes occur in the midst of the on-going war on terrorism, the operation to free Iraq, and the pursuit of Al Qaeda operatives. The FBI, for example, was called upon to interview over 10,000 Iraqi nationals and respond to elevated threat advisories four times in the last year. These have placed extraordinary requirements on the FBI, state, and local law enforcement agencies, public and private sector institutions, as well as our citizens, to take extra precautions and to increase their vigilance.

Mr. Chairman, throughout all of these fast-moving changes, the FBI has been re-positioning itself to not only remain our premier law enforcement agency, but also become our primary instrument to provide information on, and to prevent, terrorism.

OVERALL ASSESSMENT OF FBI REORGANIZATION

Mr. Chairman, the FBI has embarked on a wholesale transformation, not just a major reorganization. This transformation changes the business model in which the agency was conceived and developed. The most fundamental shift is from responding by investigating a myriad of federal crimes after the fact to preventing terrorism, espionage, and cyber crimes before the fact. This shift is driving major institutional change. The FBI's traditional system of decentralized management of localized cases is no longer adequate. In many national cases, increased headquarters management, greater headquarters-field coordination, and expanded cooperation are essential. Greater contacts with its domestic and international counterparts and extensive information exchange with federal, state, and local law enforcement agencies and the nation's foreign intelligence community are vital.

Simultaneously, the FBI's relationships with other federal, as well as state and local, law enforcement entities are changing. These entities are assuming greater responsibility for some aspects of traditional law enforcement. The FBI must, however, continue contributing both its specialized skills and extensive national and growing international networks to support their work. If this new division of responsibilities is to be successful, strong cooperative relationships with the rest of the law enforcement community will be essential.

Mr. Chairman, clearly the FBI's changing role in counterterrorism, national security, and law enforcement must be built on a strong foundation. One important building block is an extensive and robust information network. Modern communications and information processing technologies are needed not only to "connect the dots," but also to facilitate timely exchanges of massive amounts of information and intelligence. To succeed in this critical area will require major changes in many areas, including the FBI's strong institutional history of cultural independence, its personnel and training, its use of technology, and its pattern of external relationships.

There are several early signs of success in this transformation:

- First, headquarters and field personnel are highly energized; they are embracing, not resisting, change. They seem to accept Director Mueller's restatement of priorities. There are, of course, concerns about potential increases in violent crimes and drug trafficking, but not to the point of challenging the new direction.
- Second, the FBI is continuing to acquire top-notch outside talent, successfully incorporating them into its workforce, and accommodating differing perspectives in its workplace. Individuals with critical skills in information sciences, technology, intelligence, security, and administration were recruited from the private sector or have transferred from other government agencies.
- Third, resources are being allocated to reflect the new priorities. Dollars and people are now flowing to the FBI's most critical needs in counterterrorism, counter-intelligence, information technology, cyber crimes, and security. This trend is clearly reflected in the FBI's requested resources for FY 2004.

In short, Mr. Chairman, the FBI shows every sign of embracing the changes consequent to the traumatic events of 9/11, acquiring key managers and the other skills needed to implement these changes, and devoting resources in those areas fundamental to its transformation. Director Mueller is to be commended for successfully communicating his vision of a "new" FBI to the Bureau's agents and support staff, for instilling a new sense of mission and dedication, and for opening new lines of communication both internally and externally.

While these early signs are encouraging, let me temper our assessment with some words of caution. Institutional transformations do not occur overnight and involve major cultural change. Our review has focused on the FBI's near-term actions. But, many important tasks will continue for years into the future—acquiring needed personnel, developing strategies, designing plans, building systems, initiating effective operations, measuring performance, evaluating progress, and solidifying relationships with federal, state, and local agencies, and foreign governments. Mission-specific strategies, policies and doctrines, career service structures, and field unit organizations need to change. Actions are underway in many of these areas. And, with careful planning, the commitment of adequate resources and personnel, and hard work, the FBI's transformation should be well along in three or four years, though it will take longer to fully accomplish its goals. While this timetable may be longer than we all would like, with it comes the promise of significantly improved counterterrorism and information exchange capabilities.

KEY AREAS OF THE PANEL'S REVIEW

Mr. Chairman, now I would like to move to the five areas that the Panel believes are fundamental to the FBI's transformation. These are counterterrorism, intelligence, information technology, re-engineering projects, and advanced science and technology. Success in these areas should lead to successful transformation. Changes in other important areas, such as security, records management, and investigative technologies, will tend to be driven by developments in the five fundamental areas, rather than the other way around. Finally, there are two areas—the infrastructure protection aspect of its cyber division and drug enforcement—

where the Bureau's role is diminishing, as other agencies take on increased responsibilities.

Counterterrorism

Counterterrorism is the centerpiece of the FBI transformation and the driving force behind many of the restructuring and process re-engineering projects currently underway. The rationale is well known—the need to re-orient the FBI to combat terrorism by penetrating domestic cells, by preventing terrorist acts, and by investigating and facilitating prosecution of its planners and participants. Director Mueller's strategic priorities clearly place these tasks above all others.

The priority assigned to counterterrorism had already been increased by Director Freeh subsequent to the World Trade Center bombing in 1993 and to the Oklahoma City bombing in 1995. In retrospect, it's easy to see that the increased priority did not take hold. After painstaking and successful investigation of these events, field resources reverted back to more traditional priorities—violent and organized crime, drug trafficking, infrastructure protection, and counter-intelligence. Additional intelligence analysts were added, but the analytical staff

was poorly trained, had limited experience, lacked needed information and processing tools, and was easily diverted to operational support activities.

After 9/11, Director Mueller perceived, and, the Panel believes, correctly, that the FBI's decentralized case-oriented management approach no longer matched the national character of the threats from terrorist organizations. These organizations were international in scale, reacted to global interests and events irrespective of borders, addressed national targets, and operated secretively and subversively. He directed headquarters to assume management responsibility for, and oversight of, counterterrorism investigations. He also began the process of expanding the Bureau's international connectivity, improving interagency coordination at the federal level, and increasing interchange with state and local authorities.

Since 9/11, the FBI has made solid progress in structuring and improving its counterterrorism operations and the intelligence support functions in the new Counterterrorism Division (CTD).

- CTD expanded its functional units and developed new headquarters teams composed of both agents and embedded analysts well suited to address possible terrorist threats. These teams are organized by major threat groupings irrespective of the geographic area of their activities.
- About 400 field agents were reprogrammed to counterterrorism with this Subcommittee's approval. Even with this increase, actual use of field agents for counterterrorism is exceeding this revised level of 1,850 by about 1,000 personnel in FY 2003. The number of intelligence analysts, both at headquarters and in the field, is also increasing dramatically—from 159 in 2001 to 347 planned in 2003. And, an initial FBI cadre of about a dozen analysts is now supporting the new TTIC.
- Two flying squads of headquarters-based CT specialists were created, providing additional expertise, global reach, and broader perspective, while reducing the drain on field resource during emergencies. Members of these units have been deployed to 26 locations, including 14 international deployments, for example, those supporting

investigations of recent bombings in Saudi Arabia and Morocco.

- The number of Legal Attaché (Legat) offices was increased from 35 to 46 to provide increased connectivity abroad. These new locations were selected to provide improved opportunities to coordinate counterterrorism activities and exchange information with foreign law enforcement.
- A centralized 24/7 Counterterrorism Watch Unit was formed as "threat" central. At the federal level, it is supported by a new interagency National Joint Terrorism Task Force, composed of representatives from over 30 agencies, to help marshal foreign intelligence and federal information sources in response to potential threats. The FBI has also installed a major new investigative data warehouse that includes virtually all counterterrorism case files from the last 10 years, as well as translations of captured documents from Afghanistan and, more recently, Iraq.
- At state and local levels, Joint Terrorism Task Forces (JTTFs), including one at each of the FBI's 56 field offices, have been established to marshal local resources in investigating leads, respond to threats and warnings, and provide threat information to headquarters. Since 9/11, the number of JTTFs has expanded from 35 to 66 and the number of participants has more than quadrupled from 534 to over 2,300.
- Direct electronic connectivity between the JTTFs and FBI headquarters became operational in March 2003 through the Bureau's new Trilogy network. Most federal and local participants are also electronically linked to their home agencies. The FBI is currently pilot testing a prototype information sharing system in St. Louis for rapid data searching and information exchanges based on established characteristics among federal and local jurisdictions. Additional information sharing systems were funded in the Emergency Supplemental, including one for Washington DC, and more are requested in FY 2004.
- Intelligence analytic support, particularly for counterterrorism, has improved substantially. Daily Presidential threat briefings are conducted, and 30 longer-term analyses and a comprehensive national terrorist threat assessment have been completed.
- Referrals of terrorists for prosecution have increased by four-fold—from 390 to over 1,800—since 2001. Actual prosecutions and convictions have increased by similar amounts. Terrorist cells have been broken up, their financing operations dismantled, hundreds of suspected terrorists tracked, charged, or deported, and terrorist acts prevented.

- Finally, the FBI has assumed from the Department of Justice the responsibility for the continued operation of the Foreign Terrorist Tracking Task Force, an interagency collaborative effort that checks foreigners against government and commercial data bases. Under the Air Transportation Safety Act, for example, foreign flight training candidates are screened using this system, and over 30,000 individuals have been vetted.

The Panel believes this is a significant list of accomplishments. It puts in place many of the building blocks of a key part of the FBI's transformation, that of combating terrorism. It is, however, premature to claim eventual success. Much remains to be done:

- The priority of CT must be engrained in the entire organization. It cannot be seen as a transitory priority of the day.

- CTD is in the process of defining a long-term strategy to accomplish its objectives. It will be the key element in the FBI's strategic plan. The pace of progress is critical here, for this strategy will guide both the direction of the CT efforts and provide measures to judge CTD's success.
- The number of agents assigned to CT will sort itself out as workloads dictate, but support and analyst personnel need to continue to be hired and trained.
- The TTIC must be staffed to provide for comprehensive information exchange and analysis.
- Finally, the planned 2004 collocation of a significant portion of CTD with the Director of Central Intelligence's (DCI's) Counter Terrorism Center (CTC) and TTIC must be effectively implemented.

In addition, there are factors affecting CTD's development that are outside the FBI's control, notably the evolution of DHS. DHS' analytic role, its field units, and their interaction with state and local governments, especially with respect to information sharing and crisis response, may impact CTD significantly.

With respect to counterterrorism, the Panel has the following concerns:

- First, there is a real danger that, when CTD is moved outside of current FBI headquarters building, this separation could exacerbate differences between the FBI's national security missions and its law enforcement activities to the detriment of both CTD and other Bureau components.
- Second, the sharing of information and exchange of perspectives within TTIC and among collocated CTD and CTC personnel is unquestionably advantageous. But the FBI also needs to maintain its analytic independence. Critically important intelligence judgments must not be obscured by bureaucratic tendencies to compromise to the lowest common denominator. Strong, highly competent analytic capabilities are vital here.
- Third, there are increased risks in stretching the statutory authority of either the FBI or the intelligence community. The FBI is best suited to address terrorism prevention and law enforcement in the United States. Most other intelligence community agencies are properly focused on foreign intelligence. The increased sharing of information across these divides should not obfuscate this clear division of responsibilities. These are, and need to remain, clearly defined, and not left to *ad hoc* construction.
- Finally, Mr. Chairman, the FBI can't connect all the dots if it doesn't have all the dots in the first place. Clearly, the FBI has increased its information exchange with state and local law enforcement and the level of coordination and cooperation with the CIA has improved significantly. But, in the course of our review, no clear picture emerged on information sharing. The fact is we just don't know how much information is being shared, for example, between the FBI and the National Security Agency, the Defense Intelligence Agency, and other community components—though we can be reasonably assured it's not everything.

The Panel recommends that:

- **The FBI's Counterterrorism Division, irrespective of its location, remain closely coupled to the FBI Director and the rest of the FBI.**
- **The FBI develop explicit performance measures for counterterrorism that can be used by the Bureau, the Administration, and the Congress to gauge progress. While the FBI's updated strategic plan is expected to address performance measures, expert assistance might be especially helpful in developing these. If possible, these measures should include the number of terrorist attacks prevented.**
- **The FBI adopt an explicit strategy to address information sharing, establish the organizational connections, and measure progress that can confidently provide assurance to Congress that this is occurring. This will require the active cooperation of other intelligence and law enforcement agencies, but is one worth aggressively pursuing.**

Intelligence

The FBI's 2002 reorganization provided for a major increase in analytical intelligence support. A small administrative office of intelligence under the FBI's Executive Assistant Director for counterterrorism and counterintelligence was also planned, though the specific functions of that office were largely undefined. Earlier this year, the Director decided to elevate that office under a new Executive Assistant Director for Intelligence (EAD/I), subject to approval. The new Office of Intelligence is planned to be a small, but important, focal point for intelligence management supporting all of the FBI's key operational directorates. The new EAD/I-designate and the Assistant Director for the office of intelligence were only recently appointed. Plans for this office's functions and responsibilities are only beginning to be developed, and are far from being realized at this point.

As currently envisioned, the new intelligence office would have the following key intelligence responsibilities:

- Managing the FBI's intelligence career structure for analysts and other intelligence personnel. These include both intelligence personnel directly supporting operations and a new cadre of reports officers who will be responsible for preparing field-generated intelligence reports based on agent-collected information. Since 9/11, FBI headquarters analysts have produced almost 1,000 such reports for external dissemination based on field inputs. Report generation will gradually shift to field units as reports officers are hired and trained. Less than a dozen have completed their training to date, and these are currently being deployed.
- Establishing an intelligence requirements management system. This system would identify information needs and assess the state of available information. It would also identify the intelligence, law enforcement, or other agencies to be assigned to respond to these needs.
- Evaluating the responsiveness and effectiveness of both internal FBI and external collection efforts.

According to FBI officials, the intelligence office will be the interface with intelligence community activities as well as the focal point for FBI interaction with the Director of Central Intelligence's community management staff. Finally, the intelligence office plans to serve as an advocate for intelligence collection technologies and analytical tools applicable to FBI tasks, operate the multi-purpose Foreign Terrorist Tracking Task Force's data search system, and maintain a small office of senior analysts who will be responsible for agency-wide intelligence assessments.

The FBI's intelligence improvements to date have been focused on the high priority counterterrorism area. Therefore, it is not surprising that the longer-term structural and administrative aspects of the intelligence office are still being designed. It is clearly premature to judge the success of these early efforts. But many are critical to the success of coordinating intelligence community and law enforcement efforts in CT as well as other mission areas.

With respect to intelligence, the Panel recommends:

- **Requirements definition and collection assignment receive top priority in the FBI's new intelligence office. The FBI's traditional approach of referring leads to other FBI units is not a good model to emulate for intelligence collection needs. A close coupling between the disparate intelligence requirement and assignment mechanisms of the intelligence community and those needed by the FBI for terrorism prevention and law enforcement is essentially a new endeavor. It will be extremely complicated, but potentially highly rewarding.**
- **The Office of Intelligence establish a collection evaluation process that assesses those requirement and assignment alternatives most likely to satisfy information needs. In the long run, this process will be the most important aspect of judging the contribution and value of sources. And, with the President's emphasis on performance measurement, it is an increasingly important one.**
- **The Office of Intelligence remain a small staff component that aggregates the Bureau's management functions related to intelligence. At a minimum, it will be important to isolate operational and analytical tasks, so that their immediacy does not detract from the office's broader management functions. It might be better to assign such tasks to other elements of the Bureau.**

Information Technology

Last year, I highlighted information technology as a particular area of concern. The FBI was far behind other organizations. For example, in the summer of 2002, the FBI's e-mail service could not be used to communicate externally. And the basic system used to support FBI cases, the Automated Case System (ACS), relied on obsolete technology and suffered from significant security and information control weaknesses. Ineffective use of technology was a significant weakness in carrying out its traditional role and would seriously constrain its new pre-emptive counterterrorism role. Trilogy and its new case management software, Virtual Case File (VCF), were key initiatives designed to deal with these problems. The Panel believed that they needed to be watched closely.

In May of 2002, Director Mueller made upgrading the FBI's information technology one of his major priorities. To help, he brought in a number of outside experts. In the last 12 months, the FBI has deployed 22,000 new desktop computers. In March of 2003, a high-speed communications network, including 2,612 switches and routers, 622 local area networks, and 291 servers, was installed. Both of those efforts were completed on schedule. Together they provide the backbone of the FBI's new internal processing capabilities. The next phase of Trilogy, implementation of the VCF software, is scheduled in two increments. The first is to be delivered in December of 2003, and the second in the summer of 2004. According to FBI officials, both increments are on schedule.

The FBI has also started taking advantage of modern information technology in other areas. It is building a new investigative data warehouse known as Project SCOPE, and has acquired commercial software to assist its intelligence analysts' search through that data. The Bureau has loaded most of the counterterrorism files from ACS into the data warehouse and is rapidly loading other data of interest, such as that captured in Afghanistan and Iraq. This technology has already improved the FBI's ability to analyze terrorist information. I should add that the new data warehouse is designed to fit seamlessly with VCF.

In addition to energizing Trilogy and implementing SCOPE, the FBI has begun addressing the longer-term policy and organizational changes needed to help assure the future infusion of information technology. In the policy arena, it will no longer develop systems in-house and contractors are directed to make maximum use of commercial off-the-shelf products. The Bureau is also in the early stages of revising its investment management process to better assure that new acquisitions, including those in information technology, will have a significant return on investment. This responds to criticism in a December 2002 report by the Department of Justice Inspector General.

While the Panel is encouraged by the early indications of success, they are just that—early indications. Much remains to be done in this difficult and dynamic area. The FBI is just catching up to where most other Federal agencies are. Hence, while the progress is encouraging, the jury is still out on the Bureau's success in taking full advantage of modern information technology to fulfill its mission.

With respect to information technology, the Panel has the following concerns:

- The most challenging part of Trilogy? implementation, acceptance and effective use of the VCF software? lies ahead. The contractor has closely coordinated with agents in the design and development of the VCF software, but it is not yet clear whether the software will perform as expected.
- Training agents in the use of the new software, and gaining their acceptance of it will be critical to the success of Trilogy. The training and the implementation of the software have not yet begun.
- Trilogy is a necessary step in the Bureau's efforts to make use of modern technology, however, it is not sufficient for the long run. The technology used in Trilogy will need to be regularly modernized.

- The Bureau's effort in the past year was focused on the immediate need to implement Trilogy, but there is also a need to plan for strategic future use of information technology. The Bureau has begun working on establishing organizational structures and processes to assist in such planning, but they are still being sorted-out.

With respect to information technology, the Panel recommends:

- **The FBI maintain Trilogy as a state of the art system through on-going modernization and annual funding for upgrades.**
- **The FBI hire a well-qualified CIO and strengthen the role of the CIO's office. A nation-wide search for a new CIO is in progress; the new CIO should help the Bureau put in place an investment management process and identify, prioritize, and take advantage of future opportunities for the strategic use of information technology.**
- **The FBI document and maintain the FBI's enterprise architecture[1] to help assure future IT investments fit into the Bureau's strategic plan.**

The FBI's Re-engineering Projects

In our testimony last year, we urged the Director to adopt a systematic management approach to its proposed reorganization. Specifically, we recommended a three-step strategy to include (1) explicit time schedules and progress measures on implementation, (2) performance measures to be used to assess how well the reorganization's goals are being met, and (3) an annual external review to assess the FBI's progress in reaching its organizational goals. The FBI initiated a series of 40 re-engineering projects to change business processes in conjunction with the reorganization, and created a process to track progress. Further, additional projects may be generated as the initial ones are completed.

We believe that these are healthy and positive signs. The re-engineering project approach provides for leadership buy-in, active participation by implementing components, and independent monitoring by the FBI's Office of Inspection. Coordination team members from the sponsoring component and representatives from supporting components and the Inspection Office develop detailed project plans, including deadlines and deliverables. They report progress on a regular, usually weekly, basis.

The 40 re-engineering projects address an array of organization and process re-engineering areas. One category covers future workforce issues, such as recruiting, hiring, training, career development, and succession planning. Another is strategic planning and the operational strategies applicable to counterterrorism, counterintelligence, cyber, and criminal investigations. GAO has worked closely with the FBI on these two areas and is reporting separately on them. Other areas include:

[1] An enterprise architecture is a blueprint for defining and controlling the integration of systems and their components. Conceptually, an enterprise architecture is to an organization's operations and systems like a set of blueprints is to a building.

- headquarters processes, such as project, personnel, and asset management
- headquarters and field organizational design and structure
- technology, including communications, information technology, and analytical tools
- culture, values, communications, and policies

The FBI has completed 6 re-engineering projects, and 8 additional ones are at the final stage of executive management review and approval. A full list of these projects and their status is in Attachment B.

After approved for implementation, progress and performance continue to be tracked. Project plans often include measures of performance, and the FBI is working with OMB on others. These measures of performance, as opposed to measuring the progress of the re-engineering projects, are not fully developed. Also, many current performance measures are input-oriented, tied to acquiring the key personnel, staff, and other resources. Output performance measures are expected to be included in the FBI's strategic plan and the operational strategies that are under development.

With respect to the re-engineering process and its projects, the Panel recommends:

- **The re-engineering process should continue to be used to stimulate management action and monitor progress. The projects are a valuable means of focusing management attention on areas important to the reorganization.**
- **Performance measurement receive increased emphasis as the personnel and structural prerequisites of the Bureau's reorganization are put in place. We have suggested some output and outcome performance measures in the areas that we reviewed, but there has been little time to collect performance data, given the demands of the reorganization.**
- **Follow-on re-engineering projects, including one that lowers the administrative burdens on special agents, be adopted.**
- **The Bureau obtain continued assistance in developing output and outcome-oriented performance measures. Outside expertise and perspectives help ensure that measures focus on these important parameters, rather than inputs. The FBI would be well served by institutionalizing processes that encourage the Bureau to articulate its goals and experts to contribute their viewpoints.**

Advanced Science and Technology

The Panel was not formally asked to review the FBI's access to and use of advanced science and technology. However, our review involved several areas—such as information technology, cyber intrusions, and investigative technologies—that are characterized by rapid technological advance. Technology in these areas has made and continues to make major advances applicable to criminal investigation and the work processes associated with information collection, processing, and analysis. As the Panel reviewed these areas, it became increasingly aware that advanced technologies are useful to a wide range of Bureau activities. The Engineering Research Facility has become an increasingly vital part of the FBI's effort to improve its use of computer-based evidence, communications, cryptography, and genetic forensics in its arsenal of techniques.

Nonetheless, the legacy of the past suggests that the FBI's insight into, and receptivity to, advanced technology merits continued vigilance. There are indications that the press of current business, including that associated with transformation, makes it difficult to keep pace with technological change. The Investigative Technologies Division, for example, finds that the demands of wiretaps under the Foreign Intelligence Surveillance Act, computer forensics, and electronic support activities consume most of its resources. Similarly, the demands of acquiring and fielding Trilogy and VCF limit the ability of the information technology components to pursue technological improvements. New technologies—such as biometrics, facial recognition, and encryption—are likely to develop rapidly, partly as a result of the increased security concerns. There are similar developments applicable to the FBI's forensic laboratory.

Given this perspective, the Panel is pleased to note two recent developments. First, the FBI, at the direction of this Subcommittee, is in the process of establishing a Science and Technology Advisory Board composed of distinguished technical experts. Defense, DHS, and most of the intelligence community agencies use similar groups to keep themselves abreast of commercial technological developments in information processing, sensors, analytical developments, and identification and security techniques. Second, the FBI has hired a new chief technology officer from outside the Bureau and is in the process of selecting a new chief information officer.

With respect to advanced science and technology, the Panel recommends:

- **The FBI increasingly use these new mechanisms to foster an active dialogue with the private sector and other government agencies on the applicability and use of advanced technologies. These mechanisms should include the CTO and CIO positions, the recently formed Investigative Technologies Division, the Laboratory Division, and the proposed new Science and Technology Advisory Board. The Panel believes it valuable to maintain channels open to external advice and insights.**
- **The FBI consider adding a technology appendix to its strategic plan. This appendix should address the major technologies affecting its mission and the processes by which it plans to monitor commercial and other governmental advances in these technologies. Research supporting investment decisions in these technologies, possibly in conjunction with other law enforcement agencies or the intelligence community, should also be pursued.**

AREAS SUPPORTING TRANSFORMATION

We believe the areas discussed above are fundamental to the FBI's transformation, but there are several support areas that are critical to the success of this transformation and also highly dependent on it. These include areas such as security, records management, and investigative technologies. In addition, some functions formerly performed by the FBI, such as cyber threat and warning analysis and infrastructure protection, are in the process of being transferred to

DHS. Finally, other agencies, such as the Drug Enforcement Administration and state and local law enforcement entities, are increasingly expected to assume a greater share of law enforcement responsibilities in areas such as drug enforcement.

Security

The impetus for the FBI's reorganization of its security functions followed the revelation of internal security weaknesses exploited by Robert Hanssen. Prior to Hanssen, security depended heavily on personal trust among agents. Responsibilities were scattered and decentralized among the FBI's field units and within headquarters. Personnel security, national security intelligence, information security, and physical security operated separately and were managed as compliance tasks, usually assigned as collateral duty to career FBI agents.

Director Mueller created the Security Division (SecD) in December 2001 and appointed a career CIA security officer as Assistant Director. This reorganization formally implemented the basic structural and organizational changes recommended by the Webster Commission that conducted an external review of FBI security during the latter half of 2001. It found that security functions were fragmented, understaffed, and poorly coordinated and identified deficiencies in organization, policy, analysis, workforce, and performance measures that were critical to improving FBI security. Creation of SecD consolidated resources from Criminal Justice Services, Information Management, field offices, and other components within Management and Administration to direct subordination under, or programmatic management by, the SecD. These included FBI polygraph resources, the FBI Police responsible for physical and facility security at key facilities, information security specialists, and most of those responsible for personnel and document security.

The establishment of SecD accelerated progress on a significant number of security issues while the reengineering and transformation of the FBI and its work processes was underway. Its achievements are numerous, including:

- Development of a detailed five-year security program plan to knit together a patchwork of security activities through coordinated planning and increased professional security personnel. SecD's security plan is thorough, tied to programs and resources, and has been updated to take into account changing threats.
- An organizational structure adaptable to growing mission requirements has been designed and functions assigned to three separate sections:
    - personnel security for security investigations and reinvestigations, including units to analyze the investigative process and conduct polygraphs,
    - information assurance for security certification and assurance management of computer systems,
    - security operations for physical, document, and technical security functions.

  The ultimate objective is a fully-staffed division, growing from the current three to five sections by 2006 that would include separate protective security and policy, planning, and program sections.
- New policies on polygraphs and financial disclosure. Additional resources are being acquired to conduct up to 5,000 polygraphs per year, and training of clearance

adjudicators has been improved.

- All 144 new and legacy systems at headquarters are in a process of being certified and accredited. A comprehensive IT security architecture is being designed, and an enterprise security operations center is being built.
- New special compartmented information facilities and other secure work areas have been greatly expanded, and access controls improved. A security compliance unit has been created and partially staffed, and a security incident reporting system is under development.
- SecD has grown significantly in funded staff positions, from 74 in March 2001 to 475 in March 2003. Skilled security professionals have been acquired on detail from other agencies on an interim basis, and a professional FBI security cadre is being recruited and trained to assume the security duties now preformed by detailees and agents.
- A limited set of performance measures were established for FY 2003, but measures dealing with attributes such as employees screened, status of clearance backlogs, and information and physical security measures still need to be developed.

SecD has made an excellent start, but much remains to be done.

- Employment and security investigations and reinvestigations need to be consolidated to help streamline the clearance process. Automation of the security process, possibly through the Office of Personnel Management's e-Clearance initiative, needs to be aggressively pursued.
- Effective information security for Trilogy and the FBI's integrated data warehouse has yet to be demonstrated. Further, the operational imperatives for Trilogy increase the risk of premature acceptance. The Bureau is planning to do extensive training of field personnel to compensate for the near simultaneous development and deployment of these systems, but that training has yet to begin.
- The problem of balancing security and need-to-know is a complex one, and clear FBI policies and associated technical controls are required. It is not clear that the ACS and VCF have incorporated an appropriate balance, particularly in light of the wide access enjoyed by non-FBI participants in joint task forces.
- A team has been assembled to address risk management issues associated with wireless technology, but policies have yet to be defined.
- Manual provisions on security are being reviewed and a new security policy and procedures manual needs to be developed.
- The number of personnel vacancies remains large, and personnel shortfalls and facility space are the acknowledged obstacles holding back faster implementation of the security plan.

With respect to security, the Panel recommends:

- **SecD accelerate the development and approval of professional career tracks for security personnel. These will become increasingly important in the competition to attract and retain qualified security personnel.**
- **SecD be responsible for system security certification, while system users be assigned responsibility for accreditation. All systems need to be examined and certified.**

- **SecD issue a comprehensive security policy and establish a security incident reporting system that systematically identifies and tracks security shortfalls.**

Records Management

The reestablishment of a separate Records Management Division (RMD) was stimulated by significant records management problems in several high profile cases, most notably, the belated discovery of records relating to the Oklahoma City bombing case. You may recall that the Attorney General was forced to postpone Timothy McVeigh's execution pending review of these records by the defense counsel. As a result of that problem, and a subsequent report by the Department of Justice's Inspector General that documented a host of factors contributing to the problem, the FBI realized that its records management practices needed significant improvement.

The potential benefits from improved records management are much greater than the savings to be achieved through internal efficiencies. As Director Mueller has said, records management is at the heart of the FBI's integrity as a law enforcement organization. Further, improved records management should lead to more effective searches and improved internal and external sharing. Thus, the effective implementation of records management will be an important factor in the FBI successfully performing its enhanced counterterrorism role.

RMD was reestablished to ensure executive direction and full-time oversight over records policy and functions, and to consolidate all records operations to ensure consistency, thoroughness and accountability. It was created by combining three separate components of other FBI offices: the Information Management section from the Information Resources Division, the Freedom of Information and Privacy Act section from the Office of Public and Congressional Affairs, and a small, analytic unit from the former Investigative Support Division. The initial steps were underway before May 2002, when the Director announced the reorganization. The identification of resources for RMD was included in the FBI's June 2002 reprogramming action. When it was created, however, RMD was over-staffed by 86 individuals. This was resolved through attrition and by assigning personnel to increased reimbursable work.

The vast majority of RMD's resources are used to perform several routine, but important records management functions, including FBI records checks and responses to Freedom of Information Act and Privacy Act requests. The demand for FBI records checks has increased dramatically since the attacks of 9/11. In FY 2001, there were 3.2 million requests, but, by FY 2002, they had risen to 9 million. Requests for FOIA/PA have remained at about 15,000 per year. This year, RMD has started measuring the timeliness of its response to these inquiries.

The Bureau recognizes that the long-term success of records management is tied to automation efforts. Consequently, it is working to assure that records management is an integral part of such systems. For example, the implementation of Trilogy's new VCF in December of 2003 will change the way records are captured. RMD is working closely with the Trilogy office to assure VCF technology improves records capture.

RMD is also working closely with the CIO and the Assistant Director for Information Resources to improve the digital capture and effective use of records. For example, RMD is taking advantage of newer scanning technologies to improve the digitization of paper records in support of critical activities, such as analysis of terrorist-related documents seized from Afghanistan and other countries. Since October 1, 2002, RMD has scanned 4.4 million pages of such documents.

With respect to records management, the Panel has the following concerns:

- It is critical that the Bureau digitally capture information both in ACS and in VCF when it is deployed. The technology allows such records capture, but agents must make judgments about what is to be captured. In the past, agents have opted not to enter records into ACS.
- Most federal automated systems are redundantly mirrored by a paper system of official records. The Bureau can realize substantial savings by eliminating that paper system, if its VCF records are the official system of records, and those records are adequately backed-up.

With respect to records management, the Panel recommends:

- **RMD issue an electronic records management policy as soon as possible, preferably before deployment of VCF.**
- **RMD work closely with the Trilogy office on implementation of VCF to:**
    - **Assure that agent training for use of VCF stresses the need for records capture.**
    - **Maximize case management records captured in VCF as the Bureau's official system of records.**
    - **Monitor VCF use to assure that appropriate records are being captured.**
    - **Assure that records are adequately backed-up.**
- **RMD encourage greater records capture in ACS until it is phased out.**

Investigative Technologies

In the June 2002 reprogramming, the FBI established a separate Investigative Technologies Division (ITD), under the Executive Assistant Director for Law Enforcement Services, to consolidate telecommunications, computer, and other advanced investigative technologies. The new division was established because of the increased workload associated with electronic technologies, their increasing importance in investigations, and the need for the FBI to be aware of commercial technologies that impact its activities and to incorporate advanced technologies into its investigative capabilities. These electronic technologies are seen as extremely important to many FBI investigations, but are especially critical to the new counterterrorism role. A separate ITD also substantially eased the wide span of control in the Laboratory Division[2] where these sophisticated functions had been previously located.

ITD has made considerable progress on structuring its functions, filling vacancies, and

[2] The Laboratory Division continues to be responsible for collecting, processing, and analyzing evidence; providing evidence-collection training; and conducting forensic research and development.

coordinating its activities with other FBI components:

- ITD has implemented three new sections: (1) Cyber Technology, (2) Technical Operations, and (3) Electronic Surveillance, and key personnel have been selected. It completed an internal review of all components and activities to address the span of control issue.
- It has filled two-thirds of the 73 vacancies identified in November 2002 after the division structure was approved with a funded staff level of 609 personnel.
- It is working to minimize potential overlap with the Bureau's new Cyber Division. As currently structured, ITD performs forensic analyses of computers to determine technically what is on the computer and to ensure its integrity for use as evidence in court. Cyber Division conducts the content analysis to determine whether a crime has, in fact, been committed.

The division's workload continues to increase dramatically. The number of forensic searches increased from 969 in FY 2000 to 1,241 in FY 2002. The number of forensic examinations increased from 2,906 to 4,609 during the same period. Given the increased use of computers in criminal activities, the FBI expects more than 60 percent of its caseload will soon require at least one computer forensic examination.

ITD is also using communications interception techniques and systems to increase the Bureau's ability to collect evidence and intelligence. Foreign Intelligence Surveillance Act collections have increased from under 1,000 lines per year in FY 1999 to 5,000 lines per year in FY 2002. During the same period, digital collection lines have also increased from under 1,000 lines per year to over 5,000 lines per year. Meanwhile, conventional criminal Title III wiretaps have remained steady at an average of 900 lines per year.

In addition to providing operational support for current investigations, ITD is expected to work with partners in private industry to ensure that future technologies will meet the FBI's needs. ITD's ability to perform this proactive role, however, is limited by the substantial demands of providing operational support to existing investigations. ITD agents and support personnel spend most of their time providing technical help to agents and analysts in the field and keeping abreast of current technological changes. ITD recognizes the importance of future technologies—such as encryption, biometrics, and facial recognition—to the FBI's mission. But the personnel resources and other approaches to accomplishing this task are extremely limited. According to ITD, it is difficult to justify diverting scarce resources from current operational support to explore future technologies that may or may not provide useful tools and techniques.

With respect to the Investigative Technologies Division, the Panel recommends:

- **The Bureau establish a mechanism for anticipating and exploiting future technologies in such rapidly evolving areas as telecommunications, information processing, encryption, and personnel identification.**
- **ITD work closely with Science and Technology Advisory Board to fashion programs and studies that improve the Bureau's awareness of and access to future technologies. At noted earlier, Director Mueller is in the process of creating this**

board to advise on advanced science, technology, and other matters of special interest.

Cyber Division

In last year's reprogramming, a new Cyber Division was created through a consolidation of the Bureau's National Infrastructure Protection Center (NIPC) and the cyber-based criminal investigative activities previously assigned to national security, white collar crime, and violent crime units. The division's function is to "coordinate, supervise, and facilitate the FBI's investigation of those federal violations in which the Internet, computer systems, or networks are exploited as the principal instruments or targets of terrorist organizations, foreign government-sponsored intelligence operations, or criminal activity and for which the use of such systems is essential to that activity." The creation of DHS, and the transfer of NIPC to this new department, has had a significant impact on the Cyber Division.

The Cyber Division has made substantial progress in structuring its operational sections, defining a cyber crime strategy, and transferring functions assigned to DHS:

- It established and staffed four of its planned five sections: (1) Cyber Crime, (2) Computer Intrusion, (3) Special Technologies and Applications, and (4) Operational Support. A fifth section—Outreach, Capability, and Development—is planned, and a section chief has been named. The Division is in the process of forming three additional units subordinate to these sections. They will deal with innocent images, cyber action teams, and a public/private alliance.
- The Cyber Division's strategy has been developed and approved by the Director. It provides a proactive approach to preventing national security and criminal cyber threats through intensified covert cyber operations, an expanded intelligence base focused on actual cyber threats, and by leveraging multi-agency resources through integrated projects. The Cyber Division is working with OMB to develop output and outcome performance measures.
- The Cyber Division reached agreement with DHS on the transfer of positions, personnel and funds, consistent with the provisions of the Homeland Security Act. Existing FBI personnel are temporarily reporting administratively to DHS and continue to perform most of these functions. A total of 307 positions (153 agent and 154 support positions) and $55 million are being transferred to the DHS in FY 2003. These included 91 headquarters positions primarily associated with the threat and warning functions formerly performed by NIPC, and 216 field positions devoted to education and outreach efforts associated with critical infrastructure protection. Only 20 NIPC headquarters employees have actually left to work for the new department, and none of the FBI's field-based personnel have done so.
- And, as noted earlier, the Cyber Division and the Investigative Technologies Division are working to minimize any potential overlap in their functions.

Using the FBI's traditional law enforcement measures, the Cyber Division's workload, unrelated to its counterterrorism responsibilities, is increasing dramatically. Computer-associated crimes involving children through enticement and pornography are growing rapidly, and the number of cases and convictions has increased. The number of cases opened grew from 113 in FY 1996 to 2,370 in FY 2002. The number of convictions and pre-trial diversions grew from 77 in FY 1998 to 646 in FY 2002.[3] Similarly, the total number of Internet fraud complaints referred to enforcement agencies are increasing exponentially—from 6,087 in FY 2000 to 48,242 in FY 2002.

The Cyber Division hopes to use the headquarters and field personnel currently occupying the positions transferred to DHS to increase the size its investigative workforce and to implement new public/private alliance capabilities both at headquarters and in the field. The division believes it needs this capability to maintain close contacts with private companies in order to understand their vulnerabilities as a prelude to investigating intrusions and other cyber crimes. These functions were formerly part of the FBI's InfraGard program, and the extent to which DHS will assume these functions as part of its work on the analysis of the cyber threat and its outreach activities to industry is unclear.

The Cyber Division is proposing to establish a cyber intelligence and analytical capability to develop tactical analytical products to help agents with their cases at the field level and strategic analytical products that identify common threads and linkages among separate cases. Such a capability would allow ITD's computer analysis and response teams to concentrate on their core responsibility of performing forensic analysis of computer media evidence. This capability would also benefit investigative agents who are often presented with large volumes of data obtained during cases that require analysis and synthesis.

With respect to the Cyber Division, the Panel is concerned that a substantial growth in the cyber crime workload seems likely to continue, and the FBI needs an improved methodology to assess this workload, the effectiveness of its cyber crime investigative techniques, and its resulting personnel needs.

Further, the Panel recommends that:

- **Cyber Division engage in a long-tern collaboration with DHS, particularly its Information Assurance/Infrastructure Protection directorate. DHS has been charged with assessing cyber threats and vulnerabilities, while the FBI investigates cyber crimes. The activities of the division's proposed public-private alliance elements must avoid duplication of those aspects of the INFRAGARD program, which are the process of being transferred.**
- **Cyber Division continue to work with ITD to minimize duplication, particularly between a proposed cyber intelligence analyst cadre in the Cyber Division and the analysts in ITD's computer analysis and response teams.**

Drug Enforcement

Drug enforcement has been a major area of FBI program growth since the 1980s. The number of investigations that led to drug convictions grew from less than 100 in 1981 to over 3,900 in 2001. Drug convictions amounted to less than 1 percent of total FBI convictions in 1980, but

[3] Data on convictions and pre-trial diversions from FY 1996 and FY 1997 were not available.

grew to over 28 percent in 2001. By the late 1980s, drug control and enforcement operations began to account for the largest number of FBI convictions and referrals. By 2000, drug convictions exceeded the combined total number of bank robberies and bank fraud convictions, the other two top FBI enforcement activities in that year. The total number of FBI personnel (agent and support) devoted to drug enforcement increased to over 5,500 personnel in 2000, including over 2,080 agents.[4]

After 9/11, a large number of FBI personnel were assigned to support the 9/11 investigation and to assess potential terrorist threats. The Director reprogrammed 518 field agents from criminal investigative activities to counterterrorism. This included 400 from drug enforcement. Subsequently, an additional 167 drug enforcement personnel were reprogrammed to counter-intelligence for a total reallocation of 567 personnel away from drugs.

The federal government's drug control strategy places roughly equal emphasis on the demand and supply sides of the drug equation. Demand reduction efforts through drug treatment, prevention programs, and research consistently receive about 45 to 50 percent of total drug-related expenditures. The remaining 50 to 55 percent is spent on supply reduction efforts, including international crop reduction, border interdiction, and law enforcement programs.

The federal law enforcement portion of the drug control program has been spearheaded by the Drug Enforcement Administration (DEA) and the FBI. In contrast to a greater emphasis placed on marijuana cases by Customs and most other federal agencies, the FBI and DEA focus heavily on hard drugs, particularly heroin, cocaine and crack, and especially on the large international and domestic drug trafficking organizations. DEA accounts for about half of this effort, and the FBI accounts for about 15 to 20 percent. A variety of other agencies and criminal justice programs, including those in support of state and local government drug enforcement efforts, are responsible for the remainder.

A comparison of FBI and DEA referrals for prosecutions, actual prosecutions, and convictions seems to confirm the similarities of the FBI's and DEA's drug targets.

- Over 95 percent of DEA and FBI prosecutions are under the same statutes.
- The success rate of prosecutions and convictions by DEA and FBI are similar, with about 80 percent of the cases referred for prosecution actually being prosecuted, and about 75 to 80 percent of those resulting in convictions.
- Median and average prison sentences of 60 to 80 months are also similar.

In addition, the Department of Justice coordinates drug law enforcement under a system of task forces led by US Attorney's offices that include both DEA and FBI participation. These Organized Crime Drug Enforcement Task Forces include a consolidated list of priority targets that guide both DEA and FBI operations.

[4] In comparison, immediately prior to 9/11, less than 1,700 FBI personnel, including about 1,050 agents, or about 6 percent of the FBI's total staff of 27,000 worked on counterterrorism activities. In addition, there were less than 30 convictions for internal security (counter-intelligence & terrorism) in 2001

For FY 2002 and for the first six months of FY 2003, FBI drug enforcement, as measured by referrals for prosecution, actual prosecutions, and convictions, has diminished significantly—by as much as 15 percent in terms of new referrals in 2002. Reductions in the level of FBI-initiated prosecutions and convictions have been more modest as investigations and cases initiated prior to 9/11 continue to proceed through the courts. Preliminary data for the first six months of 2003 indicate that FBI referrals for prosecution are declining at about the same 15 percent annual rate. The reduction in terms of referrals for prosecution, actual prosecutions, and convictions is continuing, with projected full year 2003 levels down an additional 15 percent. (See Attachment C.) This probably reflects on-going reallocation of FBI agent personnel and agent-related support personnel from drug enforcement.

It is more difficult to determine the extent to which DEA may be picking up the additional workload as FBI resources devoted to drug enforcement decline. DEA referrals for prosecution and prosecutions rose modestly from 2000 to 2002, but convictions increased by 15 percent. This is in spite of personnel reductions during these years. The enacted fiscal 2003 appropriation provides for a DEA personnel increase of over 10 percent and a further increase of 3 percent has been requested in 2004. These increases, when realized, may be correlated with increased DEA drug enforcement referrals, prosecutions, and convictions in the future.

With respect to drug enforcement, the Panel recommends:

- **The impact of the FBI's reduced effort on drug trafficking continue to be tracked for further evaluation. The impact might show up either as increased quantities, reduced prices, or increased purity. This is an appropriate area for additional research to help determine the need for and size of future drug enforcement efforts.**
- **In so far as the Congress or the Administration seeks to retain the current level of federal drug enforcement, DEA resources be increased to offset FBI reductions. DEA personnel and other resources seem to be substitutable for FBI personnel and resources devoted to drug enforcement.**
- **The FBI maintain an active role in drug enforcement because drug trafficking is often closely related to other criminal activities, including terrorist activities and organized crime. Furthermore, drug informants are often useful sources in investigations of other crimes.**

ADDITIONAL AREAS OF CONCERN

Before concluding, the Panel wants to highlight two additional areas of concern that were not part of our review, but are fundamental to the Bureau's transformation? information sharing and cultural change.

Information Sharing

Information sharing is pivotal if the FBI is going to become the lead domestic agency in preventing terrorism, perform its other national security functions, and retain its status as the nation's premier law enforcement agency. It needs to become a routine part of headquarters-field operations within the FBI. Externally, it must be a two-way street where the FBI and the intelligence agencies exchange intelligence, and the FBI and other law enforcement agencies share information on terrorism and many case investigations. As noted earlier, this is particularly critical in counterterrorism. But it extends to other national security concerns such as counterintelligence and cyber crime as well. It also applies to criminal cases, though sharing is often limited to law enforcement entities. The Bureau, in the Panel's view, deserves high marks in this regard for broadly sharing threat information, building information bridges to the intelligence agencies and state and local law enforcement, collaborating with foreign law enforcement components, and opening itself up to external reviewers. Nonetheless, maintaining this commendable record will be a continuing management challenge. It will require constant reinforcement through training, collaboration, and cooperation in intelligence, investigative and law enforcement operations, and preemptive actions. The Panel addressed the problem of information sharing and exchange through its observations and recommendations in virtually every area, but we want to reiterate its overriding importance in transforming the Bureau.

Cultural Change

The second area is closely related—the changed culture and values that must accompany the FBI's transformation. The traditional values of the FBI agents as independent and determined must rapidly transition to include the values of joint collaboration, interagency cooperation, and information sharing. The historically strong comradery among FBI agents and the Bureau's reputation for integrity and professionalism may make these changes seem difficult. But, it is these very characteristics that should help the FBI's transformation succeed. The changes in culture and values need to be buttressed with leadership training and assignments putting that training into practice and reinforced by resource allocations that recognize these new values. This new landscape will not be familiar, and the transition will not always be smooth. But, from it, a new model of the FBI can emerge, one much better equipped to meet the nation's current needs.

Mr. Chairman, that concludes my prepared statement. My colleagues and I would be pleased to answer any questions you and other members may have.

ATTACHMENT A

PROJECT PANEL

Dick Thornburgh, *Chair*—Counsel, Kirkpatrick & Lockhart, LLP. Former Under Secretary General, Department of Administration and Management, United Nations; Attorney General of the United States; Governor, State of Pennsylvania; U.S. Attorney for Western Pennsylvania; Assistant Attorney General of the United States, Criminal Division.

Robert M. Alloway—Director, National Leadership Task Force on Y2K. Former Professional Staff Member, Subcommittee on Government Management, Information and Technology, U.S. House of Representatives; President, Alloway Incorporated; Assistant Professor, Sloan Graduate Business School, and Research Faculty, Center for Information Systems Research, Massachusetts Institute of Technology; Director, Management Information Systems, First National Stores.

Frank J. Chellino*—Criminal Justice Consultant; Former Special Agent in Charge, Miami Field Division, U.S. Drug Enforcement Administration (DEA); Vice Chairman, Executive Committee, Washington/Baltimore High Intensity Drug Trafficking Area. Prior Headquarters positions with DEA: Deputy Assistant Administrator, Office of Inspections; Unit Chief, Office of Security Programs. Prior positions with DEA: Special Agent in Charge, Washington Division Office; Supervisory Senior Inspector, Public Information Officer, Special Agent, Miami Division Office; Special Agent, New York Division Office.

Martin C. Faga—President and Chief Executive Officer, The MITRE Corporation. Former positions with The MITRE Corporation: Executive Vice President and Director, Department of Defense Federally Funded Research and Development Center; Senior Vice President and General Manager, Center for Integrated Intelligence Systems; Member, Technical Staff. Former Assistant Secretary of the Air Force for Space; Director, National Reconnaissance Office, U.S. Air Force; Professional Staff Member, House Permanent Select Committee on Intelligence.

Kristine M. Marcy—Consultant, McConnell International, LLC. Former Chief Operating Officer, Small Business Administration; Senior Counsel, Detention and Deportation, Immigration and Naturalization Service; Assistant Director for Prisoner Services, U.S. Marshals Service, U.S. Department of Justice; Associate Deputy Attorney General, Office of the Deputy Attorney General, U.S. Department of Justice; Acting Director/Deputy Director, Office of Construction Management and Deputy Budget Director, U.S. Department of the Interior; Deputy Assistant Secretary, Office of Civil Rights, U.S. Department of Education; Assistant Director, Human Resources, Veterans and Labor Group, U.S. Office of Personnel Management.

Robert J. O'Neill, Jr.— Executive Director, International City/County Management Association. Former President, National Academy of Public Administration; County Executive, Fairfax County, Virginia. Former positions with the City of Hampton, Virginia: City Manager; Assistant City Manager for Administrative Services; Management Systems Coordinator; Management Intern; Director, the Public Employment Program. Former Director of Management Consulting Services, Coopers and Lybrand; Regional Manager, Management Improvement Corporation of America.

Harold H. Saunders —Director of International Affairs, Kettering Foundation. Former Fellow, American Enterprise Institute and The Brookings Institution. Former positions with the U.S. Department of State: Assistant Secretary for Near Eastern and South Asian Affairs; Director of Intelligence and Research; Deputy Assistant Secretary. Former Staff, National Security Council.

** Not an Academy Fellow*

ATTACHMENT B

THE FBI"S RE-ENGINEERING PROJECTS

Project Name	Description of Project	Status
Career Development/ Succession Planning	Establish an FBI Succession Planning Process	Pending Approval
Trilogy	Upgrade the FBI's IT system (Transportation Network, Information Presentation, and User Applications components)	Doing Analysis
Analytical Tool for IA's	Create a data warehouse with advanced analytical tools for intelligence analysis.	Doing Analysis
FBI Culture/values	Identify policy changes, values and themes needed to align the FBI culture with the new mission, and a strategy for making those changes.	Doing Analysis
Continuity of Operations	Establish, coordinate and implement a COOP for the FBI to include identification of full-time staff	Doing Analysis
HQ Organization Structure	Restructure FBI HQ to improve decision-making, facilitate information sharing, and to provide assistance and value added support to operational divisions	Developing Plan
TS/SCI LAN	Establish and provide a secure network for communication between the FBI and other National Security Organizations	Pending Approval
Strategic Planning Process	Design a new planning process that will align management, operational, business and IT processes with strategic priorities	Pending Approval
Project Management	Consolidation of project management services within the FBI	Doing Analysis
Office of Professional Responsibility	Reorganize and to some extent restructure the penalty phase of the disciplinary process.	Doing Analysis
Training	Assess training for support, agent, and management personnel and the optimal organization structure and resources required to support the training mission.	Completed
Asset Management (property, inventory)	Establish and strengthen the FBI's accountability of government owned property, both real and personal property.	Doing Analysis
Time Utilization Record Keeping (TURK)	Determine and make changes to reform the FBI's primary workload measurement system, known as TURK	Completed
Hiring	Streamline the FBI's hiring process with a noticeable reduction in timelines.	Developing Plan
Space - HQ Long Term Strategy	Identify ways to obtain and fund space more quickly to be responsive to the FBI's need.	Developing Plan
Inspection Process	Refine the focus of inspections to ensure executive management is provided with insightful and actionable documentation	Completed
Field Office Organizational Structure	Test functional design of field offices and make recommendations for any alterations and field-wide implementation	Doing Analysis
Criminal Informant Program/Asset Program	Make specific recommendations for change in the administration of the Informant and Asset Programs	Pending Approval
Recruiting	Incorporated into the Hiring Re-engineering effort.	N/A
Records Management Division Organization	Establish a new organizational structure for RMD to eliminate duplicative functions by combining similar functions	Doing Analysis

Project Name	Description of Project	Status
Technology Tools - STARS	Develop on-line IT equipment ordering system, Standardized Acquisition Request System (STARS)	Completed
Counterterrorism Strategy	Incorporated into the Strategic Planning Re-engineering effort.	N/A
Counterintelligence Strategy	Incorporated into the Strategic Planning Re-engineering effort.	N/A
Cyber Strategy	Incorporated into the Strategic Planning Re-engineering effort.	N/A
Criminal Investigative Strategy	Incorporated into the Strategic Planning Re-engineering effort.	N/A
Fitness/Height-Weight Standards	Examine and make recommendations concerning standards of fitness testing and body fat thresholds and of reinstituting mandatory fitness testing for agents	Pending Approval
Communication Strategy	Institute a communication strategy to provide information regarding Re-engineering efforts	Developing Plan
Vital Records	Establish a program to protect records essential for the FBI to conduct critical functions or necessary to protect the rights and interests of the Government and the public	Doing Analysis
Security Manual Pilot Project	Establish a separate, stand-alone Security Program Manual	Doing Analysis
MAOP/MIOG Update	Simplify and improve access to the Manual of Administrative Operations and Procedures (MAOP) and the Manual of Investigative Operations Guidelines (MIOG)	Doing Analysis
Financial Audit Streamlining	Automate the auditing process	Pending Approval
Legal Attaché assignment preparation	Determine what changes should or should not be made to ensure an optimal level of training is provided to FBI employees for overseas assignment	Pending Approval
AO Position Upgrades	Examine the Administrative Officer (AO) position and quality control procedures in-place to ensure AOs are competent	Doing Analysis
Executive Secretariat	Establish a centralized Office of the Executive Secretariat (OES) to manage Executive level correspondence	Doing Analysis
Supplies Purchase and Distribution	Streamline the ordering of routine office supplies for all FBI, Field Office, and Headquarters divisions.	Completed
Rapid Start/ICON (major case automation)	Capture the information collected in major cases and make it available over the FBI's Intranet to all approved personnel for query/reporting	Pending Approval
SCOPE	Incorporated into the Analytical Tools for IA's Re-engineering effort	N/A
Automated Response & Compliance System	Develop an automated system to track and report external audit compliance and follow-up with oversight directives, recommendations, and requests	Completed
Analyst Professionalization	Analyst Career Development Strategy (selection, training, and promotion)	Doing Analysis
Repository for OPR/ Appeals/ Security Violations	Create a central repository for Office of Professional Responsibility (OPR), appeals to the inspection division, security violation investigations, fitness for duty, and whistle blower complaints	Doing Analysis

ATTACHMENT C

FEDERAL DRUGS AND NARCOTICS ENFORCEMENT

The table below provides further data on the importance of the contributions of DEA and FBI to the federal law enforcement portion of the war on drugs and the trends discussed above.

Federal Drugs and Narcotics Enforcement:
Selected Fiscal Years

Action	1986	1990	1995	2000	2001	2002	2003*
Referrals Total	20072	31975	34160	41369	41178	41473	20291
DEA	11403	14381	16205	20011	19708	20496	10326
FBI	3013	4124	5534	7012	6757	5789	2473
Other Federal	5656	13470	12421	14346	14713	15188	7492
Prosecutions Total	**14959**	**23994**	**25632**	**31986**	**32753**	**32850**	**15726**
DEA	**8663**	**11327**	**12489**	**15457**	**15645**	**16069**	**7886**
FBI	**1847**	**2682**	**3909**	**5014**	**4884**	**4350**	**1857**
Other Federal	**4449**	**9985**	**9234**	**11515**	**12224**	**12431**	**5983**
Convictions Total	9741	16407	15966	23289	25969	26750	13079
DEA	5629	8082	7649	10895	12200	12573	6399
FBI	1286	2084	2333	3665	3904	3753	1780
Other Federal	2826	6241	5984	8729	9865	10424	4900

* For six months of FY 2003 (October, 2002 through March, 2003).
Source: Transactional Records Access Clearinghouse, Syracuse University

It shows the rapid growth of the FBI’s drug enforcement efforts between 1986 and 2000, and provides significant evidence that FBI’s drug enforcement activities continued to expand even after Director Freeh raised the priority associated with terrorism as a result of the World Trade Center bombing of 1993 and the Oklahoma City bombing of 1995. FBI referrals for prosecution, case prosecutions, and convictions roughly doubled between 1986 and 1995 and experienced further increases of 25 to 60 percent between 1995 and 2000.