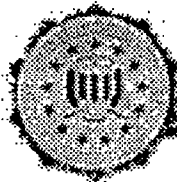


FBI Press Room - Congressional Statement - 1999 - President's Fiscal Year 2000 Budget

Page 1 of 13



Congressional Statement Federal Bureau of Investigation

March 24, 1999

Statement for the Record of
Louis J. Freeh, Director
Federal Bureau of Investigation

on
President's Fiscal Year 2000 Budget

Before the
Senate Committee on Appropriations
Subcommittee for the Departments of Commerce, Justice, and
State, the Judiciary, and Related Agencies
Washington, D.C.

Good morning, Mr. Chairman and members of the Subcommittee. I welcome this opportunity to appear before the Subcommittee to discuss the President's fiscal year 2000 budget request for the Federal Bureau of Investigation (FBI). I am also pleased to be joined by my colleague, Administrator Tom Constantine of the Drug Enforcement Administration.

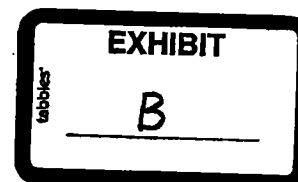
I am most appreciative of the support the Subcommittee has provided the FBI over the past several years. That support, in terms of the additional staffing and resources provided, allows us to do what the FBI does best: catch criminals, drug traffickers, terrorists, and spies; provide training, investigative assistance, and forensic and identification services to our law enforcement partners; and develop new crime-fighting technologies and techniques.

This past year, the FBI celebrated its 90th anniversary. We acknowledged that occasion by reflecting upon the successes of our past and by dedicating ourselves to carrying the FBI's proud heritage into the future. Having reached the mid-point in my tenure as Director of the FBI, I want to be sure that the Bureau of the 21st Century is rooted solidly upon our successful past and that our mission and priorities, as well as our core values and competencies, prepare us for the challenges of today and the years to come.

Challenges Facing the FBI

Before discussing our fiscal year 2000 budget request, I would like to highlight for the Subcommittee several of the challenges facing the FBI, and the strategic planning and management initiatives that we are undertaking to prepare the FBI to enter the 21st Century. These initiatives are especially important given the challenges and changes facing the FBI.

Increasingly, the crime problems and national security threats facing the FBI are transcending the traditional investigative programs under which the FBI operated. For example, the Southwest Border and East Caribbean crime plans are based upon a coordinated attack against drug traffickers (organized crime/drugs program), violent crimes and gangs (violent crimes program), and public corruption (white-collar crime program). Emerging criminal enterprises from Eastern Europe and Eurasia tend to be involved not only in "traditional" organized crime activities, such as extortion, loan sharking, and street crime, but also complex money laundering, tax evasion schemes, medical fraud, and other "white-collar" offenses.



We are also facing a growing internationalization of crime. Increasingly, cases being worked by FBI Agents on the streets of America are developing leads that take us to foreign lands for resolution. Recent events, such as the abductions and brutal murders of Americans in Uganda and Colombia, required the FBI to exercise its statutory extraterritorial jurisdiction and deploy investigative teams overseas. Organized criminal enterprises are often involved in related illegal activities on several continents. Communications networks allow criminals in foreign countries to commit thefts in the United States without leaving their homelands.

To respond to these types of emerging crime problems and national security issues more quickly, the FBI must focus its efforts and resources along broader investigative strategies.

Another challenge facing the FBI is the changing demographics of our workforce. With respect to agents, nearly 31 percent of all FBI Special Agents have been on the job for less than five years -- nearly double the rate in 1993.

- In October 1995, 9 percent of the 8,410 on-board field investigative agents were at the GS-10 entry level; by February 1999, the percentage of GS-10 entry level agents has nearly doubled to 17 percent of the 9,477 on-board field investigative agents.

- At the same time, we are also experiencing a significant loss in investigative experience. In October 1995, 74 percent of the 8,410 on-board field investigative agents were at the GS-13 journeyman level; by February 1999, the percentage of experienced, journeyman agents had decreased to 61 percent of the 9,477 on-board field investigative agents.

Keeping current with the fast pace of technology and more complex crime problems and issues requires a more technically trained and competent workforce. This applies not only in terms of our investigators, but also with respect to the scientists, engineers, analysts, and other support staff who help our agents do their jobs. We are also recognizing that technically trained specialists are becoming an increasingly important part of our investigative teams. For example, this year we are requesting 79 forensic computer examiners to assist agents with computer evidence identification, collection, and analysis. I want to acknowledge the Subcommittee's assistance in providing us with the special authority to recruit, hire, and compensate persons for select critical skill positions. We will use that authority to bring on board the specialists and technical staff needed to support our investigations.

Emerging technologies present both a challenge and an opportunity for the FBI to develop new methods and capabilities for preventing and investigating crime and protecting the national security. We must be able to upgrade existing investigative techniques and technologies and to take advantage of emerging technologies to develop new capabilities to keep abreast of changing criminal problems and national security issues.

The infrastructure necessary to support the FBI also presents challenges. The FBI employs nearly 28,000 employees, located in 56 major field offices, approximately 400 smaller resident agencies, four information technology centers, a fingerprint identification and criminal justice information complex, a training academy, an engineering research facility, and FBI Headquarters. We also operate legal attache offices in 37 foreign countries. Tying these offices together are large, complex radio communications and telecommunications networks. In addition, we also operate and maintain nationwide systems and services, such as the National Crime Information Center, the Combined DNA Identification System, and fingerprint identification systems, that provide connectivity with state and local law enforcement.

FBI Strategic Plan, 1998 - 2003

This past May, I issued the FBI Strategic Plan, 1998 - 2003. This plan represents the culmination of work performed over a year's time by a strategic planning task force

under the personal direction of Deputy Director Robert M. Bryant. This group conducted strategy sessions with every FBI investigative program, both criminal and national security, and met with FBI Special Agents in Charge and other field office representatives. In doing so, the task force not only identified the strategic direction and national priorities for the FBI, but it also performed a self-assessment of the FBI's capacity to achieve these goals. This self-assessment identified deficiencies and performance gaps that must be improved or completely eliminated if we are to be successful in dealing with emerging crime problems and more challenging threats and issues related to protecting the national security. Some of these deficiencies and performance gaps can be corrected by reengineering processes and implementing policy decisions, while others will require funding and resources to mitigate.

Guiding the implementation of our national priorities is a statement of core values for performing the mission of the FBI, which I personally wrote. Briefly, the core values that I have established for FBI employees can be summarized as follows:

- o rigorous obedience to the Constitution;
- o respect for the dignity of all those we protect;
- o compassion;
- o fairness; and
- o uncompromising personal and institutional integrity.

To accomplish the mission of the FBI, we must follow these core values. The public expects the FBI to do its utmost to protect people and their rights. As I have told FBI employees, observance of these core values is our guarantee of excellence and propriety in meeting the Bureau's national security and criminal investigative responsibilities.

The FBI Strategic Plan, 1998 - 2003 identifies three major functional areas that define the FBI's strategic priorities. These three national priorities are: national and economic security; criminal enterprises and public integrity; and individuals and property. Within these three functional areas, the FBI has identified nine strategic goals emphasizing the FBI's need to position itself to prevent crimes and counterintelligence activities, rather than just reacting to such acts after they occur.

National and Economic Security. Our highest national priority is the investigation of foreign intelligence, terrorist, and criminal activities that directly threaten the national or economic security of the United States. We have established four strategic goals for this area:

- o *Identify, prevent, and defeat intelligence operations conducted by any foreign power within the United States, or against certain U.S. interests abroad, that constitute a threat to U.S. national security;*
- o *Prevent, disrupt, and defeat terrorist operations before they occur;*
- o *Create an effective and ongoing deterrent to prevent criminal conspiracies from defrauding major U.S. industries and the U.S. Government; and*
- o *Deter the unlawful exploitation of emerging technologies by foreign powers, terrorists, and criminal elements.*

Criminal Enterprises and Public Integrity. Our second national priority is crimes that affect the public safety or which undermine the integrity of American society. These investigations are often targeted at criminal organizations, such as the La Cosa Nostra, cartels and drug trafficking organizations, Asian criminal enterprises, and Russian organized crime groups, that exploit social, economic, or political circumstances. Another focus within this area is public corruption and civil rights. For this area, we have established four strategic objectives:

- o *Identify, disrupt, and dismantle existing and emerging organized criminal enterprises whose activities affect the United States;*

- o *Identify, disrupt, and dismantle targeted international and national drug-trafficking organizations;*
- o *Reduce public corruption at all levels of government with special emphasis on law enforcement operations; and*
- o *Deter civil rights violations through aggressive investigative and proactive measures.*

Individuals and Property. Our third national priority is crimes that affect individuals and property. Within this area, we will develop investigative strategies that reflect the public's expectation that the FBI will respond to and investigate serious criminal acts that affect the community and bring those responsible to justice. Our strategic goal for this area is:

- o *Reduce the impact of the most significant crimes that affect individuals and property.*

To achieve these strategic objectives, we have developed five operational support strategies that are designed to build enhanced investigative capabilities. These operational support strategies are: intelligence; information technology; applied science and engineering; management; and assistance to support our state, local, and international law enforcement partners. With respect to FBI management strategies, we were recently notified that the FBI was afforded an "unqualified" rating for the Department's Inspector General financial audit of fiscal year 1998. An "unqualified" is the highest rating an agency can receive.

For the fiscal year 2000 budget, FBI program managers used the Strategic Plan, 1998 - 2003, and the five operational support strategies as guides for developing their resource requirements. Through an integrated strategic planning and budget framework, the FBI has significantly sharpened its focus for allocating resources based upon national priorities and strategic objectives that concentrate on the most significant crime problems and threats to the Nation.

Overview of Fiscal Year 2000 Budget Request

For fiscal year 2000, the FBI is requesting a total of \$3,293,664,000 in direct budget authority, 26,519 permanent positions (11,339 agents), and 25,576 direct workyears for its Salaries and Expenses/Violent Crime Reduction Program and Construction appropriations. This request includes direct program increases totaling 268 permanent positions (60 agents) and \$109,159,000 in five budget initiatives: Information Collection and Analysis; Counterterrorism; Technology and Cyber Crimes; Law Enforcement Services; and Infrastructure.

In addition to direct funded resources, the FBI proposes a total of 2,646 reimbursable positions (454 agents) and 2,454 reimbursable workyears for fiscal year 2000. This represents increases of 89 positions for the National Instant Criminal Background Check System (NICS) and 77 positions (35 agents) for health care fraud enforcement. The fiscal year 2000 budget reflects the transfer of FBI resources previously funded under the Interagency Crime and Drug Enforcement appropriation to Salaries and Expenses.

Information Collection and Analysis

The Information Collection and Analysis budget initiative focuses upon one of the most critical needs identified by FBI program managers, namely, the ability to collect, process, analyze, and disseminate information obtained during investigations, from other agencies, and from public sources. For fiscal year 2000, the FBI is requesting an increase of 56 positions and \$48,917,000 for information collection and analysis activities in three areas: Information Sharing, Collection Management, and Investigative Information Services.

Information Sharing. Last year, the Committee supported funding for the Information Sharing program which is a critical cornerstone to all of the operational strategies

identified by the FBI in its Strategic Plan, 1998 - 2003. What the FBI needs most is to move away from its current collection of "stove-pipe" databases and stand-alone case management systems that cannot talk to each other and implement an enterprise-wide case management system. The Information Sharing project will break down those information and case management stove-pipes.

We are taking a measured approach to implementing the Information Sharing project. This multi-year information technology investment is comprised of three sequential phases, each builds upon the preceding phase. The first phase would upgrade the existing information technology architecture to support electronic case management in all FBI locations. The second phase would introduce analytical tools that will allow FBI agents, analysts, and specialists to perform high-level analysis of the information contained in electronic case files. The third phase envisions the capability of securely sharing FBI electronic case information with other members of the law enforcement and intelligence communities.

Each major phase of the project represents a separate set of functionalities and capabilities so that if funding is not available for the subsequent phases, the investment provides benefit to the FBI. While the overall cost of all three phases will require a substantial investment over several years, our future requests will be dependent upon satisfactory progress being realized in the phases funded to date.

In response to the Committee's direction, we have prepared a five-year plan for the Information Sharing project. That plan is being reviewed within the Administration for clearance and will be submitted to the Congress upon approval from the Office of Management and Budget. Until we receive your concurrence to this plan, the FBI is unable to expend any funding in 1999 to implement the Information Sharing project.

With funding made available for fiscal year 1999, including \$20,000,000 of direct appropriation and \$40,000,000 from the Department's Working Capital Fund, the FBI would begin Phase I of the plan.

For fiscal year 2000, the FBI requests a total of \$58,800,000 to continue implementation of the Information Sharing project, including a program increase of \$38,800,000. This funding would allow us to complete Phase I, which permits electronic case file capabilities with access from all FBI locations. Additionally, work would begin on Phase II of the plan to provide a common set of analytical tools to all FBI locations that would provide the electronic capability to analyze case information on a single-case basis. The availability of these analytical tools would allow FBI agents, analysts, and specialists to perform link analysis, telephone toll analysis, visual investigative analysis, geographic analysis, and the ability to analyze large volumes of data related to a single case at a single location. The Phase II ability to perform analysis on investigative case information represents a significant first step toward achieving the type of analytical capabilities needed to support the operational objectives identified in the Strategic Plan for 1998 - 2003.

Collection Management. During the development of the FBI's Strategic Plan for 1998 - 2003, virtually every program manager acknowledged that FBI intelligence analysis capabilities, across all investigative and national security programs, were deficient. Principal deficiencies most commonly cited were the absence of systematic intelligence collection requirements from Headquarters program managers to field offices, the lack of a systematic validation of sources and their information, the absence of a mechanism for sharing of information internally within the FBI across programs, and the absence of a mechanism for sharing information outside the FBI with other law enforcement and intelligence community partners based on agreed upon policies and guidelines.

The FBI Strategic Plan identifies a number of near-term actions that are already taking place to begin building an effective collection management capability. Among the steps already taken are the designation of a staff at FBI Headquarters with the responsibility for developing and implementing an organization-wide intelligence strategy. This staff is also working with the Criminal Investigative and National

Security Divisions at FBI Headquarters to develop collection management protocols and policies, a training curriculum and promotion standards for FBI analysts, and to ensure available analytical technologies are fully exploited by the FBI.

This year, we also initiated a pilot program in our Washington Field Office to develop procedures and protocols for sharing intelligence information between two programs, national security and Russian organized crime.

To further implement an effective collection management capability that will service all FBI investigative and national security programs, the fiscal year 2000 budget requests an enhancement of \$3,682,000 to hire 56 new Intelligence Operations Specialists to serve as collection management officers in FBI field offices. The establishment of these positions is a critical element of our overall intelligence strategy. In each field office, these individuals will serve as the focal point for intelligence reporting and dissemination for criminal and national security programs and be responsible for validating the reliability of sources and their information. Also requested is \$2,110,000 to build upon a prototype data analysis capability we are beginning this year that supports FBI Russian organized crime and counterterrorism programs. This effort would be adapted later to include other FBI investigative programs and crime problems and is compatible with the Information Sharing project.

Investigative Information Services. The FBI subscribes to various commercial on-line databases, such as Lexis/Nexis, Dun & Bradstreet, and others, to obtain public source information regarding individuals, businesses, and organizations that are subjects of investigations. Information obtained includes credit records, real property and tax records; boat, plane, and motor vehicle registration records; business records, including filings with the Securities and Exchange Commission and bankruptcy filings; articles of incorporation; financial information; rental records; news articles; concealed weapons permits; and hunting/fishing licenses. In 1998, more than 53,000 inquiries were made of these databases. Information from these inquiries assisted in the arrests of 393 fugitives wanted by the FBI, the identification of more than \$37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning. Over 97 percent of the inquiries made produced new investigative information for follow-up action by agents and investigators.

Subscription to these databases allows FBI investigative personnel to perform searches from computer workstations and eliminates the need to perform more time consuming manual searches of federal, state, and local records systems, libraries, and other information sources. Information obtained is used to support all categories of FBI investigations, from terrorism to violent crimes, and from health care fraud to organized crime. To meet increased subscription costs associated with accessing these public source databases, an increase of \$4,325,000 is required for fiscal year 2000.

Counterterrorism

The bombings of the World Trade Center in 1993, the Murrah Federal Building in 1995, U.S. military facilities in Saudi Arabia in 1995 and 1996, the Atlanta Olympic Games, clinics, and bars in the Southeast United States in 1996, 1997 and 1998, and, most recently, U.S. embassies in Tanzania and Kenya, are dramatic reminders of the devastation and toll in human lives that can result when terrorists and criminals use improvised explosive devices. Bombs — either conventional or unconventional — are considered the most likely threat to United States' citizens and interests from either international or domestic terrorists.

Since 1981, the FBI has operated the Hazardous Devices School, the only formal, domestic training program where state and local bomb technicians can learn to locate, identify, render safe, and dispose of improvised explosive devices, as well as learn to use specialized equipment and protective clothing needed for the safe disposal of explosive materials. With your support, the FBI has adjusted its training program at the Hazardous Devices School to meet the challenge of today's terrorist

and criminal threat, to include devices containing materials classified as weapons of mass destruction, and to train enhanced levels of bomb technicians.

During fiscal year 1998, we trained 838 state and local students through the Hazardous Devices School, including 247 in basic bomb technician courses, 152 in recertification courses, 386 in weapons of mass destruction courses, and 53 in executive management courses. We also provided basic or recertification courses for 125 FBI Special Agent bomb technicians.

For fiscal year 2000, the FBI requests \$9,000,000 for the modernization of facilities at the Hazardous Devices School, which is located at Redstone Arsenal, Alabama. This funding will be used to construct improvements related to practical exercise areas, several mock villages, and required infrastructure. These improvements and mock villages will permit bomb technician trainees the opportunity to apply techniques and training learned in the classroom in a realistic training environment. Improved facilities at the Hazardous Devices School is one of the strategies identified under the Attorney General's Five-year Counterterrorism and Technology Crime Plan that was submitted to the Congress in December 1998.

Technology and Cyber-crime

The growing use of technology by criminals, terrorists, and foreign intelligence agents to commit acts or to thwart the efforts of law enforcement investigating illegal activities is one of the serious challenges facing the FBI now and in the future. The Technology and Cyber-crime budget initiative focuses upon the resources needed to meet this challenge. For fiscal year 2000, the FBI is requesting an increase of 207 positions (60 agents) and \$36,742,000 to enhance its capabilities for preventing, detecting, and investigating computer crime and protecting the critical infrastructure of the United States.

National Infrastructure Protection Center (NIPC). The NIPC serves as a national resource for critical infrastructure protection. Critical infrastructures are those physical and cyber-based systems essential to the minimal operations of the U.S. economy and government. The national security of the United States depends largely on cyber-based systems and the rapid, consistent, secure, and reliable movement and storage of data which they provide. Presidential Decision Directive (PDD) - 63 assigns to the FBI and the Department of Justice the responsibility for the Emergency Law Enforcement services sector and lead agency responsibility for law enforcement and internal security.

The FBI supports these responsibilities through the activities of the NIPC. The mission of the NIPC is to identify and investigate threats and unlawful acts targeting the critical infrastructures of the United States and prevent illegal intrusions into government computer networks, protected civilian computers, and the national information infrastructure, consistent with PDD-63 and federal statutes. Under PDD-63, all Executive Departments and agencies are instructed to share information about threats and warnings of attacks, as well as actual attacks, on critical government and private sector infrastructures with the NIPC. The NIPC is directed to process law enforcement and intelligence information for inclusion into analyses and reports which the NIPC provides in appropriate format to other federal, state, local government agencies and private sector agencies.

The NIPC is staffed by FBI employees, as well as representatives from the United States Secret Service, the United States Postal Service, Department of Defense, Department of Energy, Oregon State Police, and others. Efforts are underway to include private sector participation in NIPC.

For fiscal year 2000, an increase of \$1,656,000 is requested for the NIPC to support training, liaison, and outreach initiatives.

Field Computer Crime and Intrusion Squads. Computers, the Internet, and other new

information technologies are an integral element of how we conduct business, perform research and development, engage in personal communications, and educate and entertain ourselves. However, as society has moved on-line, so have criminals. Crimes facilitated by the use of computers and the Internet include the defrauding of senior citizens, dissemination of child pornography, theft of credit card numbers, money laundering, insurance fraud, stock market manipulation, and theft of bank funds. On-line larceny has become a lucrative business due to the Internet's widespread availability and the growing popularity of electronic commerce.

Computers and computer networks are also the target of hackers and others who illegally gain access in an effort to deny or disrupt service, steal data, alter computer code, and plant destructive viruses and Trojan horses. A 1998 Computer Security Institute study reported that 64 percent of its survey respondents experienced a computer security breach and that losses associated with computer intrusions totaled \$136 million.

By 2000, the FBI will have established and equipped specialized computer crime and intrusion squads in 10 FBI field offices: Washington, D.C., New York City, San Francisco, Chicago, Dallas, Los Angeles, Atlanta, Charlotte, Boston, and Seattle. The FBI needs this capability in each of its field offices. To provide that capability, the fiscal year 2000 budget request includes 108 new positions (60 agents) and \$11,390,000. When combined with existing positions, it will allow us to staff and equip 18 additional computer crime and intrusion squads and to provide equipment to establish a baseline computer crime and intrusion capability in 28 smaller field offices. This request will enable the FBI to have a computer crime capability in each of its 56 field offices.

Computer Analysis Response Teams. Crucial evidence is increasingly being found in electronic form. The use of computers and computer storage media by criminals, terrorists, and foreign intelligence agents, is very well documented. The FBI and law enforcement must have the capability of recovering evidence and data from computers and computer storage media. This is becoming a very time-consuming and resource intensive process due to the growth in both the availability of computers and the size and capacity of computer storage media.

The FBI established the Computer Analysis Response Team (CART) program under the FBI Laboratory to provide data forensic services. We currently have trained and equipped 95 field CART examiners and 26 Headquarters examiners. Last year, in fiscal year 1998, these examiners conducted over 2,600 examinations. We project the demand for examinations to more than double by 2000.

The FBI is working with state and local law enforcement to share data forensic laboratory techniques and expertise. For example, we are establishing a pilot regional computer forensic laboratory capability in the FBI's San Diego field office. The multi-agency laboratory will be staffed by examiners and technicians from the FBI and state and local agencies and serve as a resource for that region. We have also developed the Automated Computer Examination System (ACES), which is an automated forensic search capability for locating computer evidence on seized computers and computer storage media. We hope to make ACES available to other law enforcement agencies.

For fiscal year 2000, the FBI is requesting \$9,861,000 to hire and train 79 new computer forensic examiners, 17 for the FBI Laboratory and 62 for assignment directly to FBI field offices and computer crime and intrusion squads, and for CART program equipment, supplies, and training. Unless we increase our capacity for performing data forensic examinations, investigators and prosecutors will be denied timely access to valuable evidence that will solve crimes and support the successful prosecution of child pornographers, drug traffickers, corrupt officials, persons committing fraud, terrorists, and other criminals.

Technical Support for Investigations. The widespread use of digital telecommunications technologies and the incorporation of privacy

features/capabilities through the use of cryptography pose a serious technical challenge to the continued ability of the FBI and law enforcement to access and process information obtained pursuant to court-authorized electronic surveillance. In today's telecommunications environment, the FBI must contend with layers of protocols, formatting, compression, and proprietary encoding applications that can have the effect of masking or hiding the content of lawfully intercepted communications. For example, the expansion of electronic commerce and concerns for privacy have brought about new concepts and deployments in affordable and robust encryption products for private sector use.

Terrorists, both abroad and at home, are using technology to protect their operations from being discovered and to thwart the efforts of law enforcement to detect, prevent, and investigate such acts. Ramzi Yousef, convicted for his role in the World Trade Center bombing and for conspiracy to destroy numerous United States airliners, used encryption to protect his computer files. Convicted spy Aldrich Ames was told by his Russian handlers to encrypt his computer files. International drug traffickers and child pornographers are using encryption to avoid detection by law enforcement.

For fiscal year 2000, increases totaling 20 positions and \$13,835,000 are requested for technical support to investigations. To handle a growing workload of requests from FBI field offices for protocol analysis and processing support for court-approved Title III and Foreign Intelligence Surveillance Act intercepts, \$6,835,000 is needed to hire and train 20 technicians, acquire technical equipment, and develop signal processing and network intercept tools to assist technicians and investigators. Additionally, \$7,000,000 is requested to develop and enhance FBI counter-encryption technology and support services that will allow law enforcement access to the plain text of encrypted communications and computer files lawfully seized pursuant to court-authorization and search warrants.

Law Enforcement Services

Later this summer, the FBI will bring on line the new National Crime Information Center (NCIC) 2000 and the Integrated Automated Fingerprint Identification System (IAFIS). Both of these systems will offer state and local law enforcement an array of new, long-awaited features and capabilities. For example, NCIC 2000 will offer the capability of transmitting a single fingerprint from a squad car to help verify the identification of a person stopped for a traffic violation. One of the features of IAFIS is a latent search capacity that will allow state and local agencies to directly submit fingerprints for matching against the FBI's database. Another key IAFIS feature is the two-hour response time to criminal fingerprint cards submitted electronically. These two systems will help us catch wanted persons and prevent the release of fugitives before their true identities can be learned. Yet, the real success of these systems depends upon state and local law enforcement possessing the equipment that will allow them to take advantage of these tools. I am hopeful that state and local governments will make these investments now that our systems are coming on line.

The Law Enforcement Services budget initiative encompasses three critical requests totaling 94 positions (5 direct and 89 reimbursable) and \$9,500,000 that will allow the FBI to provide better forensic and information services to federal, state, and local law enforcement. These items are: the implementation of the Federal Convicted Offender DNA database; improved telecommunications network connectivity between the FBI and other federal, state, and local forensic laboratories that support users of the Combined DNA Information System (CODIS) and the National Integrated Ballistics Information Network; and the National Instant Criminal Background Check System. These requests directly support the state and local assistance strategy of the FBI Strategic Plan, 1998 - 2003.

Federal Convicted Offenders DNA Database. The Anti-Terrorism and Effective Death Penalty Act of 1996 authorized the FBI to "expand the CODIS to include Federal crimes and crimes committed in the District of Columbia." No other federal agency or crime laboratory is authorized to establish such a capability. In December 1998, the FBI submitted to the Congress a plan, requested in the 1998 Justice Appropriations

Act, to support the implementation of a program that requires a federal prisoner convicted of a federal offense involving a victim who is a minor or a sexually violent offense to provide a DNA sample for inclusion in a law enforcement DNA database prior to the prisoner's release from incarceration. That report included draft legislation which requires Congressional enactment for the FBI to implement the plan. The draft legislation also clarifies the authority for implementing the Federal Convicted Offender DNA database authorized by Congress in 1996.

The FBI requires 5 positions and \$5,336,000 in fiscal year 2000 to implement the Federal Convicted Offenders DNA database. This database would include DNA samples from offenders convicted in federal, military, and District of Columbia courts. While all 50 states have enacted laws allowing the collection of DNA samples from persons convicted in state court for qualifying offenses, there is no collection of DNA samples from persons convicted in federal, military, or District of Columbia courts. Consequently, when state and local law enforcement check DNA evidence recovered from a violent sexual assault, murder, or child molestation, there are no profiles in CODIS of convicted federal offenders who may have been released and are now residing in that community. The proposed legislation and the Federal Convicted Offenders DNA database would close this gap resulting from the lack of a federal DNA collection program.

Forensic Laboratory Connectivity. One of my goals for the FBI Laboratory is the development and transition of new and improved forensic examination capabilities and crime-fighting tools to state and local forensic laboratories and law enforcement agencies. Two such tools are the National Integrated Ballistics Information Network (NIBIN) and CODIS.

NIBIN is a computer database system which allows forensic examiners within a region or large metropolitan area to exchange and match cartridge casings and bullets, thereby linking serial shootings incidents and recovered firearms. CODIS is the national DNA database system containing indices of DNA profiles from convicted offenders and unsolved crimes. CODIS permits state and local crime laboratories to exchange and compare DNA profiles electronically, thereby linking serial violent crimes, especially rapes, and identifying suspects by matching DNA from crime scenes to profiles from convicted offenders.

Growth in the number of user locations, database records, and queries is outstripping the existing capabilities of the FBI telecommunications network supporting NIBIN and CODIS. We have developed a plan to consolidate these separate networks and provide secure communications, path redundancy, and improved access to NIBIN and CODIS users. Under this plan, the FBI would migrate NIBIN and CODIS telecommunications services to the wide area network established for the Criminal Justice Information Services Division. To facilitate consolidation, an increase of \$4,164,000 is requested in fiscal year 2000.

National Instant Criminal Background Check System (NICS). The Brady Handgun Violence Prevention Act required the Attorney General to establish a NICS that any federal firearms licensee may contact for immediate verification on whether the receipt of a firearm would violate federal or state law. The NICS system became operational on November 30, 1998. Since starting operations, the FBI NICS operations center has processed more than 2 million background checks. More than 22,000 gun purchases have been denied to convicted felons and other ineligible persons. NICS has been successful in keeping guns out of the hands of criminals, while facilitating the sale of firearms to those who are not prohibited by law from purchasing a gun.

Presently, 15 states and territories serve as full points of contact for the NICS system. As such, these states and territories perform NICS checks for the purchase of both handguns and long guns. Another 11 states serve as partial points of contact for the purchase of handguns only. For the remaining 27 states and territories who are not serving as points of contact and for long-gun checks in partial point of contact states, the FBI performs NICS checks. For fiscal year 2000, the FBI estimates it will perform

approximately 6.6 million NICS checks for non-point of contact states and territories, while state points of contact will perform approximately 5 million checks.

An additional 89 reimbursable positions will be required by the FBI in fiscal year 2000 to process the projected NICS workload. The FBI's workload for NICS in fiscal year 2000 could be affected by decisions made by states serving as points of contact to cease performing that service.

For fiscal year 2000, the Administration is proposing to fund the cost of FBI NICS operations through the collection of user fees that would be paid by persons desiring to establish their eligibility to purchase a firearm. At this time, we estimate the fee will be between \$11.00 and \$13.00. We anticipate that a Notice of Proposed Rulemaking for the fee will be published in the Federal Register in either April or May. The Final Rule must be published prior to September 1, 1999, so that the fee can be implemented effective with the beginning of fiscal year 2000 on October 1, 1999.

Most recently, on March 3, 1999, the Department of Justice published a proposed rule in the Federal Register to shorten the NICS records retention period from its current six months to 90 days. This represents the minimum time period that would be needed to detect prohibited felons who assume the identity of a qualified person to buy guns illegally and to identify individuals who misuse the NICS system to perform background checks unrelated to gun purchases. Retention of records for this limited time period will allow the FBI to conduct audits that protect against invasions of privacy that could result from misuse and abuse of the NICS system. These audits are essential to safeguard the security and privacy of personal information, such as criminal and arrest histories, mental health information, and military service background information, that is part of NICS. I want to state unequivocally that the Department is not using this information to establish a national gun registry and that records of eligible purchasers will be destroyed after 90 days.

Infrastructure

The FBI anticipates awarding a contract for the construction of its new Laboratory facility at the FBI Academy in Quantico, Virginia, by mid-April. While occupation of the new FBI Laboratory will not occur until late 2001, it will be necessary to begin acquiring specialized scientific and laboratory equipment, cabling, and furnishings for the new facility in fiscal year 2000 so that these items can be installed prior to occupancy. Some specialized equipment that will be needed for the FBI Laboratory is not made on a production line; rather, it is produced on an application basis. Manufacturers require a substantial lead time to produce, test, validate, and calibrate new instruments before shipping for installation. To begin the acquisition of specialized equipment for the new FBI Laboratory, an increase of \$5,000,000 is requested.

Related Departmental Funding Requests

I would like to comment briefly on several related Department funding requests that directly affect the FBI in 2000, including: the Telecommunications Carrier Compliance Fund (TCCF), the Narrowband Communications Fund, and state and local bomb technician equipment funding.

TCCF. Within the General Administration appropriation, a total of \$15,000,000 is requested under the TCCF to continue reimbursements to telecommunications carriers and service providers as authorized by the Communications Assistance for Law Enforcement Act (CALEA).

Narrowband Communications. Also within the General Administration appropriation, an enhancement of \$45,979,000 is requested for Departmental narrowband radio equipment and services. Of this amount, approximately \$32,435,000 would be made available to the FBI for acquiring replacement hand-held, mobile, and other radio communications equipment that complies with narrowband requirements issued by

the National Telecommunications and Information Administration. Under these requirements, the FBI must replace its existing VHF radio communications equipment and system with new technology that operates on one-half the current bandwidth.

The FBI has nearly 12,400 hand-held radios and over 11,000 mobile radios that are not compatible with narrowband technology and which must be replaced. Our field offices have identified a need for nearly 3,400 hand-held radios and 3,100 mobile radios above current inventory to support FBI and task force operations. We also operate the largest, civilian land-based mobile radio communications infrastructure in the United States that will also need to be replaced to accommodate the new narrowband radio technology.

State and Local Bomb Technician Equipment. Finally, within the Office of Justice Programs, a total of \$45,000,000 is requested for the FBI to continue a program of providing chemical and biological detection technology and other equipment to state and local bomb technicians and bomb squads. This funding builds upon initiatives supported in prior years by the Subcommittee to enhance training for the bomb technician community and to train and equip these technicians and squads for dealing with large, improvised explosive devices, including devices involving chemical toxins and biological agents.

Legislative Proposals

Mr. Chairman, the fiscal 2000 budget request includes several legislative items proposed for the FBI, including: danger pay authority, foreign cooperative agreement authority, extension of the Title 5 demonstration project, and a new demonstration project for the defensive arming of a limited number of non-agent surveillance specialists.

- Section 114 would extend to me the same authority that DEA Administrator Constantine currently enjoys for authorizing danger pay for personnel assigned to high risk overseas locations. For the FBI, this is both a pay equity issue for FBI Agents assigned to DEA Country Offices and a recognition of the increased threat facing FBI personnel performing extraterritorial investigations in foreign locations due to our counterterrorism efforts. At times, FBI personnel are deployed to overseas locations where they face a threat or danger that does not always extend to all members of the United States diplomatic team in a particular country. This authority would allow me to recognize those situations.

- Section 115 would extend from three years to five years the duration of the limited exemption from Title 5 for critical skill positions. That limited exemption was granted by the Congress in 1998. An extension is needed so the operating plan for the demonstration project, which was approved by the Subcommittee in January 1999, can run for the full three years originally envisioned.

- Section 116 would allow the FBI to credit to its appropriation, funding that is received from friendly foreign governments for that country's share of joint, cooperative projects.

- Finally, Section 123 proposes a demonstration project to evaluate the feasibility of arming, for defensive purposes only, up to 50 members of FBI Special Surveillance Group teams, that provide surveillance support in counterintelligence and counterterrorism investigations. This is a safety issue. Our surveillance teams are operating in more dangerous and hostile environments and against individuals who are more unpredictable in their behavior. I am concerned for the safety of these highly trained specialists who are finding themselves in harm's way as they perform their duties in support of our counterterrorism and counterintelligence programs. The proposal includes specific safeguards with respect to qualifications, selection, training in firearms proficiency and deadly force policy for individuals selected for the demonstration project.

Last year, the Committee was supportive of several legislative provisions, including an emergency procurement authority for the Attorney General and authority to extend payments for relocation expenses for Department of Justice personnel transferred to Puerto Rico and other territories. I would like to extend my sincere thanks for your assistance on these issues, and particularly for helping us address one of the quality of life issues that we believe will help attract and retain fluent Spanish-speaking agents for our San Juan Field Office.

Summary

I am especially proud of the work being performed every day by the men and women of the FBI. Their ability to do that work is a reflection of the strong support given to the FBI by this Subcommittee. I believe our strategic vision and plan of action will position the FBI to deal with the challenges we face from increasingly complex and changing crime problems and national security threats. The budget initiatives proposed for fiscal year 2000 will help us implement our Strategic Plan and give us the opportunity to achieve the strategic objectives that we have identified for ourselves. I believe our priorities and objectives reflect the expectations for the FBI that are held by the American public, as well as the Congress.

Again, I thank you for this opportunity to appear before the Subcommittee.