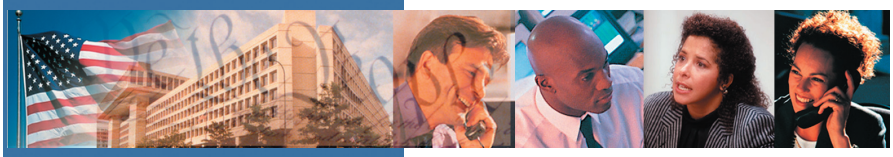
SECTION IV



TOOLS

Tools are fundamental to the FBI's ability to achieve its mission. Tools empower the FBI and its partners to gather necessary data more effectively and efficiently, convert it to actionable intelligence, and disseminate it to the parties best able to make use of it. Tools include such items as communications equipment and electronic surveillance devices (investigative technology); laboratory and psychological evaluation services (forensics); and databases and analytic software (information technology). Security is also a fundamental tool that must be fully integrated into the organization and its activities to protect our people, information, and techniques.

A. Security

Strategic Goal

Establish an enterprise-wide Security Program that protects our people, information, and capabilities.

Situation

Security is vital to the FBI's efforts to protect the United States. As the agency responsible for counterintelligence, counterterrorism, cyber, and major criminal investigations, the FBI is a high-priority target for virtually every hostile and many otherwise friendly intelligence services, terrorist organizations, criminal groups, and individuals with grievances against the U.S. Government. The nature of the threat posed by these various groups and individuals is a function of their intent, and thus varies with the particular agenda of each. Criminal groups, for example, benefit from knowing specifics of ongoing investigations. Timely knowledge of who is under investigation, which communication lines are under surveillance, or who is providing information to the government can effectively cripple an ongoing case. Because of its high visibility as a well-known element of the U.S. Government, many terrorist groups view the FBI as a desirable target for attack. Because of these threats, the Director of the FBI took immediate action to consolidate and centralize management of security programs by placing responsibility and authority for all such programs under the new Security Division. The Security Program will expand over the next five years guided by a philosophy of evolutionary rather than revolutionary change. It is assuming an oversight role in the management of security programs that were previously controlled by the field offices and the FBI Headquarters' divisions. The FBI recognizes that all security threats, vulnerabilities, and risks must be identified, assessed, evaluated, and managed using a systematic and rational process as part of a continuing operational strategy.

Strategic Objectives

IVA.1 Protect the FBI from compromise of its employees.

Security and counterintelligence professionals generally agree that the most significant threat to an organization's internal security is betrayal by a trusted insider. An individual with legitimate access who chooses to betray the FBI's trust is particularly damaging because compromise of information may continue over an extended period of time and encompass a wide range of programs. Worse, the insider can target his or her activities to compromise the information most relevant to the needs of the adversary. If undetected over a period of time, a person

could rise to a leadership position within an organization from which he or she may influence policy. To enhance countermeasures against these threats, the FBI developed, implemented, and expanded its Financial Disclosure and Personnel Security Polygraph Programs. These measures have already minimized the threat, but additional actions are needed to further protect the FBI and the nation.

Priority Actions

- Establish a Security Center of Excellence to provide expert security guidance to the FBI and its customers.
- Develop and implement the Security Division Management Information System which will document, track, and analyze data relevant to personnel security.
- Establish and communicate well-defined security policies, providing guidance that is clear and well-understood, and that facilitates compliance.

IVA.2 Protect the FBI from compromise of its communications and information.

The proliferation of information technology in recent years has resulted in dramatic changes in the threat environment. The explosion in electronic data handling has profoundly altered the manner in which most modern organizations, including the FBI, manage information. While modern technology allows the storage, movement, and retrieval of vast amounts of data to the benefit of investigators and analysts, it also allows, absent highly sophisticated security precautions, the lightning-fast theft of vast amounts of information, or the crippling of response capabilities in a time of crisis. Experience has shown that the cyber threat is typically a human problem, not a technical problem. Even though it is true that information systems and networks offer attractive targets, it is invariably the human element in those systems that make them exploitable. Information systems and networks have human involvement during the complete system life-cycle. They are vulnerable during construction, shipment, installation, operation, maintenance, and disposal. Advanced technology solutions alone will not solve the problem. The approach must be multi-disciplinary and must cover the complete life-cycle of information systems, data, and human intervention. To meet these threats, the FBI developed and implemented a Certification and Accreditation process that has been incorporated into the organization's information technology investment and development life-cycle, including all legacy systems. However, additional measures are needed to further protect the FBI from the compromise of its information technology systems.

Priority Actions

- Bring the Enterprise Security Operations Center to full operating capacity in order to detect and prevent FBI network intrusions.
- Establish an Information System Security Manager (ISSM) Program, with ISSMs assigned to all operational and major support divisions.

IVA.3 Protect the FBI from physical attack.

The unique position occupied by the FBI within the U.S. Government and in the public consciousness makes it a high priority target for terrorist groups seeking publicity, for criminal organizations wishing to intimidate or take reprisal, and for lone malcontents with specific grievances. No other federal government agency deals as directly, in what is nearly always an adversarial fashion, with the variety and number of violence-prone groups as does the FBI. Bomb threats and threats of other violence involving FBI facilities and personnel, while not commonplace, occur with sufficient frequency to generate increasing concern. There are an increasing number of threats directed at individual agents and their families as intimidation or retribution for activities carried out in the performance of their official duties. Additionally, since 9/11, increasing numbers of FBI personnel have been dispatched to areas of recurring terrorist and insurgent activities including Afghanistan, Saudi Arabia, and Iraq. The Security Division established a Risk Analysis Staff, which uses analytical risk management methodology to guide the development of threat analysis and development of appropriate risk mitigation decisions. Additional measures will be implemented to further reduce both the risk and consequences of an attack.

Priority Actions

- Establish intelligence-driven processes to proactively assess new security threats and the effectiveness of existing countermeasures, and make appropriate changes in protection strategies.
- Develop a Critical Mission Assurance Program with Continuity of Operations Planning at FBI Headquarters and in all field divisions.

B. Information Technology

Strategic Goal

Establish a secure, flexible, and modern information technology system that fully supports the collection, analysis, and dissemination of information.

Situation

Prior to 9/11, the FBI made substantial investments to upgrade technologies that directly supported investigations (e.g., surveillance equipment, IAFAS), but little attention was paid to technology related to the more fundamental tasks of records creation, maintenance, dissemination, and retrieval. As a result, the FBI's information technology infrastructure became antiquated and unable to support operations effectively. Most of the FBI's computer systems were designed at a time when the conventional wisdom and prevailing technology were that data was "owned" — collected and manipulated — in discrete systems. Such systems are now viewed as "stove-pipes" because the information stored in them cannot be quickly shared or cross-referenced. The FBI has been hamstrung by outdated technology in terms of networks, hardware, software, and infrastructure support.

Information technology requires constant upgrading in order to remain viable and flexible to changing requirements. The FBI hired experts from outside to modernize its systems. The first imperative was to develop an Enterprise Architecture . However, 9/11 created immediate critical needs to prevent further terrorist attacks. Decisions were made and actions taken to meet those exigent needs. As noted by the GAO, there are inherent risks in modernizing information technology systems without the benefit of an Enterprise Architecture. The decisions that were made took into account such risks. The FBI chose to be an early majority technology adopter with a strong bias toward purchase versus development. We selected a few key standards, and in some cases specific mainstream products, to anchor the technology portion of our architecture. Even without a comprehensive architecture, the FBI was still able to achieve enumerable successes as a result of the character and resolve of its personnel. It is imperative that the FBI have the ability to view, conjoin, and analyze data already in its possession in ways and places not previously anticipated. The FBI threat forecast predicts the continued emergence of temporal threats and the need to quickly shift to emerging threats. The FBI must be able to quickly search all in-house data or legally accessible external data, regardless of source or location, for relevant intelligence. Moreover, the FBI will need to ensure that its systems are compatible for sharing information electronically to the widest extent possible to meet the intelligence needs of our partners.

Strategic Objectives

IVB.1 Ensure all current and future information technology plans work towards a harmonized system.

One significant hurdle for all organizations moving from older to newer technology is the recognition that neither developers nor users can completely predict the ways in which the technology will be used in the future. Thus, over time, we have all learned that unanticipated technical and data connections will be needed. Such connections are not only internal to our own organization but external to it as well, as the importance of data and work-sharing rises. In order to be able to meet such requests, all technology must be included within a single, conceptual Enterprise Architecture. GAO and many other governmental entities have recognized the importance of having a single such scheme and all require explanations of how any new technology will fit within an Enterprise Architecture before approving spending or building. An Enterprise Architecture must be developed using recognized industry methodology that will best support the existing information management systems while allowing new development to benefit from the enhanced infrastructure. One of the most important hurdles that must be considered is that the FBI is not operating in a static environment. While a new Enterprise Architecture is being developed, ongoing investigations must remain largely unaffected. The Director and FBI senior executive staff are committed to an Enterprise Architecture and will interact with the Enterprise Architecture team and make decisions based on input and recommendations from the FBI's Network Architect. Lastly, a solid proven methodology will be employed to ensure that all the necessary requirements and concerns are being addressed.

Priority Actions

- Fully staff the Enterprise Architecture Core Team.
- Complete and disseminate an Enterprise Architecture Management Plan that fully addresses external data-sharing and work-sharing.
- Establish a high-level baseline architecture; high-level target architecture; initial Transition Plan and partial products.
- Complete an Information Technology Strategic Plan.
- Create a Business Reference Model, Data and Information Reference Model, Service Component Reference Model, and a Performance Reference Model.

- Establish a system that revises annually the Enterprise Architecture, Strategic Plan, and the Transition Plan.

IVB.2 Make all technology available to employees wherever they work or travel.

The FBI must provide tools that will allow it to take full advantage of surge capabilities and make additional or specialized personnel available wherever they are needed to address threats. This may mean that an employee in Phoenix will be temporarily assigned to work on an issue for Los Angeles or Headquarters, without ever leaving his or her desk. Information technology will be at the forefront of that toolset as employees will need to store the results of their collection efforts; retrieve and correlate from the larger pool of available information; and share the resulting intelligence. In order to implement this vision, all relevant information technology must be potentially accessible and transferable to any employee in any office. The FBI's Trilogy project has begun that process by upgrading to communications facilities, network servers, and desktop workstations that can accommodate the same enhanced technologies. The future challenge is to continue upgrading in order to keep pace with the technical prowess of our adversaries.

Priority Actions

- Complete Trilogy upgrades currently underway.
- Ensure a technology refresh cycle of 36 months for mission-oriented work.
- Establish and implement a plan to make all technology available to any employee at any fixed office location.

IVB.3 Build or adapt data storage and retrieval systems to permit the flexibility to respond to changing threats and priorities.

Newer database and data warehouse technologies separate storage functions from access functions, making it possible for different divisions, sections, or units to place all data in a single virtual repository and get different views of it based upon their needs. Through "extensibility," storage elements can be added later to accommodate new participants or programs. This is not without challenges. Although data need not be stored with the tool that accesses it, access technology still dictates the format it can retrieve and, therefore, the format in which data is stored. In order to work with currently available access technology (and to conform to e-gov standards), significant programming is required to make all of the data compatible. The FBI has undertaken the important effort of converting its data to XML and,

with its partners, to establish metadata standards which will facilitate data sharing. Current data access technology also requires that data be stored according to a data schema that anticipates the desired flexibility; the FBI is working towards this by creating a logical data model and offering to share it with partners. The information technology industry is working to establish mechanisms to access disparate data without these expensive and time consuming processes and it is possible that the breakthrough will come within the next five years. If so, we must be prepared to capitalize on such an advance.

Priority Actions

- Ensure all new data collection occurs in compliance with the metadata standards.
- End "stove-pipe" systems by converting all investigative and intelligence data into formats which can be accessed via a virtually linked storage facility.
- Implement new application software for field investigations and, subsequently, upgrade the software until functionality entirely replaces identified "stove-pipe" systems.
- Revise plans to take advantage of newer, more effective and efficient technologies as they are made available.

IVB.4 Provide tools to increase the speed and efficiency of data use.

Improving the tools for data access is an increasingly critical requirement. Advances in the ability to collect and store text, graphics, audio, and video data have resulted in a tremendous amount of information which outstrips the human ability for processing. Concomitant tools must be used to parse, analyze, and meaningfully report the available data. Many such tools are currently available throughout the FBI, but they need to be provided more consistently. The data tools industry is constantly enhancing its offerings, providing real opportunities to improve the speed and accuracy of obtaining results. These advances will become increasingly important as the FBI, in addressing rapidly developing threats, works to prevent events before they occur rather than solving them after they occur.

Priority Actions

- Ensure all virtually linked data can be accessed by tools which allow for analysis, visualization, and reporting of text, graphics, video, and audio data.

- Consolidate efforts in developing analytical tools and provide this capability across-the-board.
- Revise plans to take advantage of newer, more effective and efficient technologies as they are made available.
- Deliver additional tools which enable investigators and analysts to triage, exploit, and share intelligence and other information collected via electronic means.

IVB.5 Ensure that data is secure.

Data is one of the greatest weapons of our time. Because of its great power, we must ensure that FBI data is secure and available at all times. This is accomplished through both intrusion detection/protection and the creation of a viable continuity of operations plan (COOP) in the event of system disruption. While the FBI gathers and uses data in the fight to reduce the threats against our citizens, it is clear that the very same data can be turned against us as a weapon of immeasurable force. It also has the potential to be used for less disastrous but equally illegal or inappropriate purposes. As the FBI places more data in a single repository and provides more access points and views, it must be increasingly vigilant in ensuring that the data is handled in ways that are consistent with the U.S. Constitution, privacy and record-keeping laws, classification standards, and federal regulations and policies.

Priority Actions

- Ensure that a COOP is in place and updated annually to address changes in environment and technology.
- Ensure that back-up data and processing is available at regional off-site locations.
- Continue to require regular review of all information technology plans to ensure conformity to all legal standards.
- Seek to ensure that both in-house and external punishment measures for willful inappropriate use of data is commensurate with the damage caused.
- Ensure that data security tools and measures have the capacity to identify inappropriate or suspicious access, use, or dissemination.
- Ensure that data security measures keep pace with developments in tools.

C. Investigative Technology

Strategic Goal

Effectively utilize applied science and engineering resources to empower the FBI's investigative and intelligence operations and thwart the techniques of our adversaries.

Situation

In addressing today's terrorists, intelligence operatives, and criminals, computers and electronic media have become the evidentiary equivalent of yesterday's paper files. Moreover, the potential sources of audio, video, and image evidence continue to expand as technologies advance and as adversaries make wider use of them. Video cameras and other audio and imaging technologies, such as solid-state recording devices, voice mail systems, Internet audio, digital cameras, and flatbed scanners, are becoming commonplace throughout the world. The electronic surveillance (ELSUR)[2] of criminals, and of foreign powers and terrorists, has proven to be one of the most effective tools of the U.S. Government. The FBI's emphasis on proactive and preventive counterterrorism, counterintelligence, and cyber activities requires technical collection and analysis activities that adapt from historically simple technology to a more complex systems approach, resulting in the development of new tools and the retraining of investigative, translation, intelligence, and technical personnel. In June 2002, the FBI established the Investigative Technology Division in order to consolidate all responsibilities for technical investigative support and increase the emphasis on future investigative technologies.

Strategic Objectives

IVC.1 Improve the speed of access to and dissemination of information collected through data and telecommunications intercepts.

The FBI must enhance its collective capacity to expeditiously identify, understand, and take appropriate action to counteract crime problems and threats against the United States. In the furtherance of these efforts, the FBI will develop and implement tools that enable investigators and analysts to triage collected data, permitting them to crystallize actionable intelligence obtained from an ocean of collected information.

[2] There are two federal statutory regimens pertaining to electronic surveillance — one regarding criminal investigations and another regarding foreign intelligence, counterintelligence, and terrorism investigations. The former is derived from (1) Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (commonly referred to as "Title III"), as amended; (2) portions of the Electronic Communications Privacy Act of 1986, as amended; and (3) portions of the Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994. The latter is derived from the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended.

In this regard, the Investigative Technology Division has developed and deployed a system to monitor, minimize, exploit and disseminate over the FBI's TRILOGY network the product of lawful ELSUR operations in a collaborative user environment. This initial capacity will be expanded through the development and implementation of an integrated capability that enables FBI users, as well as our partners in the Intelligence Community, to process, view, analyze, and disseminate all digital evidence collected pursuant to a lawfully-authorized seizure or intercept order. Upon implementation, the Electronic Surveillance Data Management System (EDMS) will provide an enterprise web-based collection management and information retrieval capability for all FBI field offices. EDMS will automate the capability to prepare reports, locally conduct investigative analysis, and provide users with analytical tools for automated speaker identification, text key word spotting, voice key word spotting, and language identification.

Priority Actions

- Implement EDMS as means to establish a common user interface that will enable appropriate personnel to have enterprise-wide access to collected data, as well as the capacity to engage in remote collaborative and intelligence sharing activities.
- Research and implement analytic tools which will assist in the prioritization of collected material.
- As authorized by pertinent laws and guidelines, support joint exploitation of collected information by establishing an architecture for sharing collected data, comments, and analysis.

IVC.2 Improve the delivery of existing tools, technologies, and services, and develop and deliver new technologies, tools, and services to investigators and analysts.

Keeping abreast of advancing technologies is critical to empower our employees in their duties and to thwart the technical capabilities of our adversaries. The anticipated growth in the number of Internet users, continued consumer demand for broadband technologies, and the mobility associated with wireless Local Area Networks (LANs) and Third Generation Wireless systems which converge voice communications and Internet access, requires constant vigilance by the FBI. The number of broadband households in the United States is growing at a rate of about 100 percent per year, from 6.2 million in 2000 to an estimated 34.7 million by the end of 2004. This higher bandwidth access increases by about 50 percent the

volume of material looked at and, as a result, the volume of data intercepts and potential evidence also increases.

Changes in cellular technology recently caused the Federal Communications Commission to announce plans to phase out all analog systems within three to five years. Also, the increasing emphasis on digital connectivity and electronic commerce has been a catalyst for the introduction of stronger, more user-friendly data protection (e.g., encryption technology) and destruction systems. While this is beneficial for legitimate users, others have taken advantage of this technology to conceal or destroy evidence. The FBI must expand its efforts to make critical technology leaps by aggressively exploring, developing, and delivering significant new, even "generation-skipping," technologies, operational capabilities, tools, and services. These efforts include, but are not limited to, those pertaining to computer-based evidence; communications; facial recognition; audio, visual, and imaging forensics; tactical operations, and surveillance operations.

Priority Actions

- Increase the level of technical support to investigations involving intercepted electronic information employing data protection.
- Expand capacity to provide field investigators with body recorders; data and communications interception and dissemination equipment; audio sensor systems; and video equipment.
- Meet investigators' demand for physical surveillance/tracking and audio/video/image enhancement tools.
- Enhance investigators' capacity to conduct physical surveillance and tracking operations.
- Improve capabilities to compromise security and countermeasure devices confronted during entry and search operations.

IVC.3 Improve the technical ability of law enforcement to ensure intercept capabilities are consistent with private industry's advances in technology.

Several mandates have been dictated to the FBI by Congress and oversight agencies. These responsibilities include but are not limited to efforts to implement CALEA; and to vacate the microwave band from 1700 MHz to 1755 MHz as required by the Omnibus Budget Reconciliation Act of 1993.

Advances in telecommunication technologies and services have impaired the Law Enforcement Community's ability to conduct fully effective, lawfully authorized electronic surveillance operations. CALEA was enacted to preserve electronic surveillance operations as tools for investigating our nation's most serious and violent offenses. CALEA requires the telecommunications industry to proactively address law enforcement's needs and directs the industry to design, develop, and deploy technical solutions meeting certain assistance capability requirements, including capacity requirements. CALEA authorized appropriations of up to $500 million to reimburse carriers for certain "reasonable costs" in complying with the statute.

Nearly nine years after its enactment, the statute has not yet been fully implemented. The industry has not adopted the development and deployment of electronic surveillance capabilities as a basic element of providing service, and has resisted full implementation of CALEA through multiple litigations, requests for extensions, and other means. By the end of 2004, we expect only 40 percent of law enforcement priority switches to have CALEA technical solutions deployed. The FBI will work with its law enforcement partners at all levels to foster relationships with individual carriers and their respective equipment manufacturers, as well as to expand law enforcement's understanding of technologies and services where industry-setting standards do not exist or industry sectors have to date refused to develop technical standards.

Priority Actions

- Develop strategies to motivate industry to implement CALEA.
- Ensure CALEA implementation team is staffed with technically trained agents familiar with operational requirements as well as technical requirements.

IVC.4 Improve radio communications within the FBI.

The FBI has had its own dedicated tactical wireless system, the Land Mobile Radio System (LMRS), since the 1940s. Beginning in 1999, sufficient funding has not been available for maintenance or upgrades, and the system has begun to deteriorate. Some of that equipment is so dated that replacement parts are no longer available. Concurrently, the proliferation of wireless technologies has created unprecedented demand for radio spectrum which is a finite natural resource. The Congressionally-mandated narrowband communication initiative requires legacy radio equipment to be replaced with equipment using the narrowband by 2005. In this regard, the FBI must replace more than 32,000 radios, both portable and mobile. The new compliant

systems will be more technically advanced, and will offer a multitude of enhanced technical and security capabilities. An aggressive training initiative will be needed to ensure the viability of the new systems. The migration to "narrowband" is being accomplished through the joint Department of Justice — Treasury Department — Department of Homeland Security Integrated Wireless Network. Until that system is fully implemented and operational, the FBI will be required to concurrently purchase and maintain equipment for the LMRS system that is migratable to the narrowband.

Priority Actions

- Ensure the complete and timely implementation of the Integrated Wireless Network and continue to maintain the legacy LMRS in the interim.
- Provide increased level of guidance regarding the development, procurement, and installation of a secure wireless communication system.

D. Criminal Justice Information Services

Strategic Goal

Provide timely and relevant criminal justice services to the FBI and to authorized law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Situation

The CJIS Division was established to provide nationwide criminal justice information services. To meet expected increases in future demand due to programs such as civil fingerprint-based background checks for employment and licensing, and border entry activities to detect terrorists attempting to enter the United States, CJIS needs to significantly increase its systems' capacity. Future fingerprint requirements are pushing towards immediate, instantaneous responses. Additionally, law enforcement's daily NCIC transactions have significantly increased. These and other increasing demands call for the "next generation" of CJIS systems.

Automation and computer technology necessarily require constant upgrading and enhancement if such systems are to remain viable and flexible in response to changing customer requirements. As a general rule, computer capabilities double in performance every two years. Software companies constantly upgrade and enhance their software to accommodate the improved hardware. At some point, early technology versions will not work with newer hardware or software. This will result in an expensive retooling of the entire system. Inevitably, if a computer system is to remain viable, reliable, and able to meet growing customer demands, technology systems must continually upgrade.

Improving technology will also include expanding Internet usage. The transmission over the Internet of fingerprint images, Criminal History Reports (CHRs), crime statistics, gun checks, etc., provides all agencies the ability to benefit from information sharing at a lower cost than a dedicated Wide Area Network (WAN). This is an area that the CJIS Division will explore for future use.

The Law Enforcement OnLine (LEO) system has tremendous potential to meet law enforcement's growing requirements for Internet connectivity and information sharing. While LEO has been able to operate and provide an acceptable level of service, it will need to be enhanced to meet future demands.

A critical external issue that negatively impacts the CJIS is CHR accuracy. Half of the CHRs do not have a final disposition (e.g., conviction or dismissal). This

impacts the quality of information provided through the fingerprint identification, NCIC, and National Instant Criminal Background Check System (NICS) services. In the case of NICS, it consumes significant resources to retrieve dispositions in order to provide gun dealers information on an individual's qualification to purchase a gun.

In addition to the expansion of its existing services, CJIS is embarking on a major new endeavor relating to information sharing between different FBI, law enforcement, and civilian databases and information services in a manner that provides richer and more relevant information to its customers. When developed, the system will provide the ability for a single query to profile all of an individual's contacts with law enforcement. By tracking crime in real time and presenting it in a graphic representation, law enforcement can improve its analysis of criminal and terrorist activities and discern connections that previously would have been impossible.

Strategic Objectives

IVD.1 Expand information sharing capabilities to support customer needs.

An array of state-of-the-art technology in the Uniform Crime Report (UCR) Program is needed to provide more efficient, optimum quality, and timely products and services to law enforcement and other consumers of UCR crime data. The new system will optimize the production capabilities of the existing CJIS information systems by leveraging the immense amount of data already regularly contained in each system repository. It will deliver an efficient, automatic correlation of all CJIS data. Once achieved, law enforcement and national security stakeholders will have the ability to run data against other information residing on the various agency-based systems, so that the optimum level of correlations between current and past criminal and homeland security matters can be accomplished without the need for labor intensive, human intervention. The requestor would not only receive specific information based upon regular, electronic queries, but would also gain knowledge about any other law enforcement entity's actions, past or present, which has commonality with the requestor's current subject.

Priority Actions

- Conduct a pilot program of the Concept of Operations.
- Develop an implementation plan based on the results of the assessment of the pilot project.

IVD.2 Expand the National Incident-Based Reporting System (NIBRS) data fields for distribution to law enforcement and others throughout the United States.

The System of Services Information Sharing Initiative requires participants to utilize an "enhanced NIBRS" data set for the data input to support the information sharing process. This enhanced data set combines the current 53 NIBRS crime descriptors with the specific personal and event identifiers which form the core of most police department incident reports. Many states collect more information than the current 53 NIBRS data elements describing incidents for their own in-house purposes. To realize the full potential of the information sharing capabilities of NIBRS data, additional identifying data (e.g., victim, offender, and suspect) must be included, which will provide law enforcement additional investigative leads. This information will serve as a valuable tool in criminal and national security matters.

Priority Actions

- Closely coordinate with state, local, and federal NIBRS stakeholders in the development of an implementation plan.

IVD.3 Improve the availability of dispositions and other information used to evaluate individuals for firearm and other civil background checks.

Because of the lack of availability of dispositions, the FBI and the states cannot always complete the necessary firearm background checks within the legally mandated three business days. In order to improve this performance gap, the NICS Section will work to increase information sharing with state and federal agencies. This not only benefits NICS, but should also impact the overall disposition problem.

Priority Actions

- Initiate an Outreach Program to increase information availability from state and federal agencies.
- Develop and automate the Disposition Document File and any restoration of rights files submitted to the NICS Section.
- Increase Protection Order records, Felony Flags, and Brady Indicators.

IVD.4 Develop, implement, and promote the Next Generation IAFIS for fingerprint identification and criminal history information services.

If CJIS is to meet growing customer requirements, it must develop, implement, and promote the Next Generation IAFIS for fingerprint identification and criminal history services. Significant improvements in the availability and timeliness of services are required in order to share valuable criminal history information with an ever-increasing customer base in an expeditious manner. IAFIS currently provides a two-hour or less response time on electronic criminal submissions and a 24-hour or less response time on electronic civil submissions. However, customer requirements for fingerprint identification services are changing at a rapid pace. CJIS must maintain a state-of-the-art Automated Fingerprint Identificcation System technology to keep pace with the ever-increasing demands of the Law Enforcement Community, as well as the civil community. CJIS must improve and expand its ability to receive flat, ten-print fingerprint data for identification and latent purposes, as well as its ability to extract fingerprint data for export to the Department of Homeland Security for the United States Visitor and Immigrant Status Indication Technology (US VISIT) Program. For many customers, a fully electronic fingerprint process from the customer to the FBI and back has not yet been achieved. Enhanced fingerprint capabilities are also sought by the Terrorist Threat Integration Center and the Terrorism Screening Center.

Priority Actions

- Assess the status of IAFIS customers by state, federal, and regulatory agencies where appropriate. Identify customer requirements for Next Generation IAFIS.
- Implement phased testing of Next Generation IAFIS.
- Determine the feasibility of implementing a national, rapid, and positive fingerprint-based identification background check system for authorized noncriminal justice purposes.
- Complete the National Fingerprint Applicant Check System testing and field work.
- Provide IAFIS data to support the US VISIT Program.

IVD.5 Expand the availability of CJIS services using the Internet.

The Internet provides a valuable tool for exchanging fingerprint identification, criminal history, and other relevant information by improving CJIS's ability to interact with its customer base. The Internet allows CJIS to: (1) exchange data among local law enforcement agencies, courts, and other entities; (2) increase the number of dispositions on file within the CHR repository, which will enable law enforcement and regulatory agencies to make better, more timely decisions regarding issues such as employment, firearm purchases, and criminal activity; and (3) offer training at the convenience of our customers with information in real time.

Priority Actions

- Develop a strategy to use the Internet to enhance and promote fingerprint identification and CHR services.
- Initiate a feasibility study for the transmission of CHR updates via the Internet (i.e., disposition information, expungement information).
- Implement training initiatives via the Internet.

IVD.6 Expand the content and services available on LEO.

LEO's objective is to use the Internet to provide the Law Enforcement Community with an expandable, reliable Sensitive But Unclassified service for sharing information, communicating alerts, and educational purposes. Unfortunately, there are still state, local, and federal first responders without LEO's critical support services. As LEO implements its initiatives and transitions them to an operational status, improvements and enhancements will be needed. LEO will provide an Enterprise Domain for connectivity between users throughout various agencies. This expansion includes Continuity of Operations, thus, increasing LEO's reliability and availability for all users. In order to achieve these activities; however, upgrades in hardware, software, business processes, and features are needed to enhance and improve the services.

Priority Actions

- Expand LEO's services with additional antiterrorism and law enforcement features.
- Develop a management plan and supporting documentation consistent with FBI/DOJ/Office of Management and Budget approval and direction.

IVD.7 Develop and Implement a Business Continuity Plan for CJIS.

A Business Continuity Management process improves procedures and practices and increases the organization's resilience in the event of interruption or loss. It will ensure that CJIS's services will be available (proaction), and if an incident occurs, CJIS can minimize the impact to the customer (reaction). There are two aspects to this goal: the technology and the staff. The effort to protect the technology requires a significant amount of resources and planning, particularly in the case of a catastrophic event. Even a seemingly insignificant event, such as a short-term but substantial snowstorm, can impact the available staff to service customers.

Priority Actions

- Implement a Disaster Recovery System that provides business continuity for the CJIS Division's critical services.
- Develop a comprehensive contingency plan.

E. Forensics

Strategic Goal
Establish a worldwide network of scientific services that maximizes forensics in combating terrorism, cyber-based attacks, and crime.

Situation
The proper collection, preservation, and forensic analysis of evidence is a tremendous tool that must be fully exploited. Since its inception, the FBI has been the world leader in using science to solve crimes. During its first year of operation in 1932, the FBI's forensics unit conducted 963 examinations. Currently, the FBI conducts more than one million forensic examinations annually. The types of investigations addressed forensically by the FBI include terrorism, espionage, public corruption, civil rights, criminal organizations and enterprises, white collar, and violent crime. Not only has the volume of evidence received increased dramatically, but the complexity of the examination methods, as well as the complex nature of the investigations themselves have increased. Often, forensic analysis is the only means to provide conclusive information to a jury to assist them in their determination of guilt or innocence.

Forensics is also an essential tool in combating terrorism in that it provides evidence that establishes links and associations that can withstand judicial scrutiny in the United States and abroad. Moreover, comprehensive crime scene searches and the subsequent forensic analysis of evidence is sometimes the only solid intelligence that exists or the only mechanism to corroborate other intelligence reporting. FBI forensic analysis was essential in piecing together the evidence to identify those responsible for, as well as the supporters of, every terrorist attack against the United States, including the mid-air bombing of Pan Am Flight #103, the bombing of the World Trade Center in 1993, the bombing of the Oklahoma City Federal Building in 1995, the bombing of the two United States Embassies in East Africa, the attack against the U.S.S. Cole, and the 9/11 attacks on the World Trade Center and the Pentagon.

In January 2003, the American Society of Crime Laboratory Directors — Laboratory Accreditation Board (ASCLD/LAB) board of delegates voted to adopt Digital Evidence as an accreditable discipline. The Investigative Technology Division conducts forensic examinations in the discipline of Digital Evidence as defined by the ASCLD/LAB. These examinations are performed at FBI Headquarters and field offices by certified forensic examiners.

The evolving threat environment increasingly requires the rapid deployment of FBI forensic examiners to locations around the world in order to collect and preserve evidence that could otherwise be lost forever. FBI forensic resources are increasingly being called upon to support high profile criminal investigations in other countries because of the FBI's unique forensic expertise and capability. The FBI will also need to help develop the forensic capabilities of other countries and to leverage existing capabilities within the United States through partnerships with other forensic laboratories and scientists to provide the optimum level of forensic services to meet the increasing demands. It is imperative that constant improvements in forensic analysis be sought through a robust research and development program and that these improvements be quickly deployed to support the entire forensic community.

With the exponential growth of the World Wide Web, terrorists, foreign actors, and criminals are increasingly using this technology, along with encryption, to facilitate their operations. The FBI and its partners must keep up with the increasing demands required in providing timely forensic analysis of computer-related evidence in support of terrorism, foreign intelligence, cyber, and criminal investigations.

Strategic Objectives

IVE.1 Increase the FBI's ability to provide forensic analysis in support of its own investigations as well as those of other agencies.

The FBI receives an increasing volume of evidence and an increasing number of requests for expert testimony from federal, state, and local law enforcement agencies. It is incumbent upon the FBI to provide operational assistance to international, federal, state, and local agency partners. While the completion of the new FBI Laboratory provides tremendous forensic capability to assist in these matters, increasing demands over the next five years will outpace the FBI's ability to deliver timely examinations.

Priority Actions

- Complete a comprehensive assessment of the FBI's future forensic resource needs.
- Expand the use of information technology in the conduct of examinations, comparisons, and the sharing of results, as part of the FBI's information technology modernization efforts.

- Expand the forensic capabilities of the Investigative Technology Division's Computer Analysis Response Team (CART) Program and its ability to quickly share the results of computer forensic exams.

- Continue to develop the Combined DNA Index System (CODIS) as a means to assist in the identification and capture of international terrorists.

IVE.2 Increase the FBI's forensic response capabilities.

The proper collection, preservation, and forensic analysis of evidence from the scene of a terrorist attack or major crime is critically important. There is only one opportunity to do it correctly; otherwise, critical links and evidence may be lost forever. The global threat of terrorism and international crime requires a timely forensic response capability around the world. The need for these services will increase over the next five years, and the FBI must be able to meet this demand. While the most dramatic increase of services will be overseas, the FBI's forensic expertise is often called upon to address major crimes in the United States as well, including initial processing of crime scenes.

Within the first six weeks after 9/11, the FBI's CART examined more than nine terabytes (nine million megabytes) of data. With the onset of world-wide access to computers and increased knowledge within the general population, it is reasonable to expect a computer to be involved in some fashion in virtually every investigation the FBI conducts. Furthermore, the FBI is Congressionally mandated to provide computer forensic support, in addition to other forensic support, to state and local law enforcement agencies which it accomplishes through its Regional Computer Forensic Laboratory (RCFL) Program. The RCFLs are partnerships among the FBI and other law enforcement agencies within a geographic area, and the program has continued to grow since its inception with the number of labs expected to exceed 10 by the end of 2004. As such, computer forensics are expected to play an ever-increasing role in the FBI's future operations.

Priority Actions

- Increase the number of employees participating in the FBI's Evidence Response Team Program in support of international and domestic crime scene searches.

- Establish specialized Rapid Deployment Teams to conduct expeditious examinations of both computer-related and other physical evidence in support of investigations and intelligence operations.

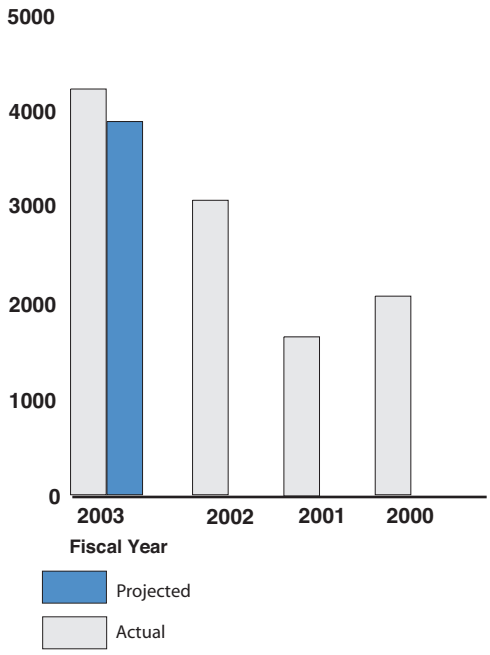
- Expand the CART Program's forensic capabilities and the ability for case investigators to review examination results.

- Develop, plan, and schedule for basic and advanced hazardous materials training to bring on line 10 additional field Hazardous Materials Response Teams and enhance the existing capabilities.

IVE.3 Increase the forensic capabilities of all law enforcement and intelligence agencies both within and outside of the United States.

FBI forensic resources are increasingly being called upon to support high profile criminal investigations in other countries because of the FBI's unique forensic expertise and capability. The FBI will need to help develop the forensic capabilities of other countries and leverage existing capabilities within the United States. This will be accomplished through partnerships with other forensic laboratories and scientists to provide the optimum level of forensic services to meet increasing demands worldwide.

Measure Refined: Total Number of Forensic and Offender Matches Identified at the NDIS, SDIS, and LDIS

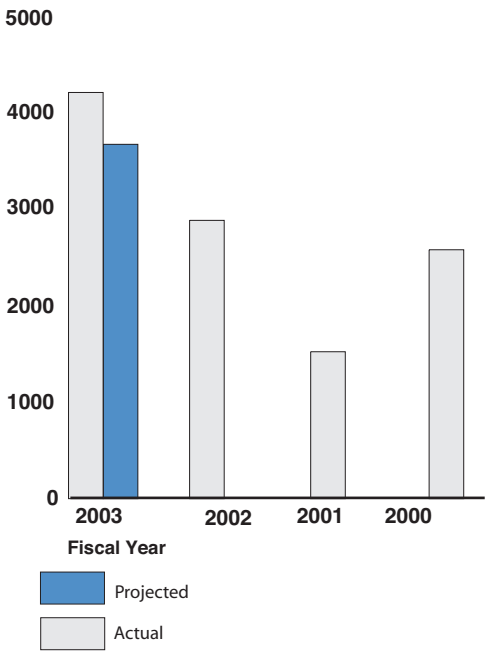


Data Definitions: NDIS, SDIS, & LDIS Matches: NDIS, SDIS, or LDIS finds a DNA match, CODIS software geerates a report that shows a match and/or "hit" has been made and then provides an offender or forensic profile based on the sample received.

Priority Actions

- Continue to provide training and certification to the FBI's state, local, and international forensic partners.
- Upgrade proficiency testing through the use of externally prepared tests.
- Expand the CODIS Program both domestically and internationally, via the Legats. Improve training and information for all CODIS users.
- Work with other federal crime laboratories to develop a Continuity of Operations Plan.

Total Number of Federal, State and Local Investigations Aided By the Combined DNA Index System (CODIS)



IVE.4 Increase forensic research and development projects.

The FBI will be able to accomplish its mission and support its priorities not only through the collection and examination of evidence, but also through continual state-of-the-art forensic science research, as well as training counterparts throughout the professional community. It is imperative that constant improvements in forensic analysis be sought through a robust research and development program and that these improvements can be quickly deployed to support the entire forensic community.

Priority Actions

- Establish joint partnerships with state and local laboratories for research and development.
- Work with the National Academy of Sciences regarding a review of bullet lead analysis.

F. Records Management

Strategic Goal
Establish a state-of-the-art record keeping system.

Situation
The FBI system of records must ensure that accurate records of all activities are created, maintained, and disposed of in accordance with all legal requirements. The system must provide timely and accurate responses to requests for information from government agencies that need FBI information to perform their mission. The system must also be responsive to requests for information under the provisions of the Freedom of Information and Privacy Acts (FOIPA). Currently the FBI has several electronic record keeping systems, but none have been approved by the National Archives and Records Administration (NARA) as a system of records. Only the paper-based, physical file has been approved as a system of records, and hence, the FBI must maintain tens of millions of paper files. This paper-based system is costly and inefficient. The FBI is modernizing its information technology systems, and a fundamental requirement is an electronic record keeping capability with unquestionable accuracy and integrity including the use of digital signatures.

Strategic Objectives

IVF.1 Establish an electronic record keeping system.

The FBI collects and produces a tremendous number of documents while performing its mission, most of which constitute official records. Dramatic efficiencies can be achieved if the FBI adopts an electronic record keeping system. The FBI's official system of records is currently paper-based and decentralized, and is maintained at 265 different locations, including FBI Headquarters, field offices, resident agencies, some Legal Attaché offices, Investigative Technology Centers, and various off-site locations. Advances in information technology provide an opportunity to dramatically improve the efficiency of this system of records, which is so critical to operational and administrative functions. A principal goal of our modernization efforts is the adoption of a Records Management Application that supports an electronic record keeping system for all legacy and future information technology systems.

Priority Actions

- Centralize all FBI records.

- Acquire and implement a Records Management Application that can address the record keeping requirements for all FBI legacy systems and the FBI's future information technology systems.

- Closely collaborate with NARA to ensure the electronic record keeping and automated record management applications meet all requirements for an electronic record keeping system.

IVF.2 Modernize the FBI's National Name Check Program.

The National Name Check Program is the FBI's system to provide information on individuals from FBI records to other federal agencies, congressional committees, intelligence agencies and other agencies that need this information to support their mission. The program historically conducted an average of 2.4 million name checks annually; however, an increased emphasis on homeland security has resulted in an exponential increase in requests. It is anticipated that the number of requests will continue to increase over the next five years at a rapid rate. Hence, the FBI must achieve dramatic improvements in the National Name Check Program to meet customer demands. This can only be achieved through information technology and improved processes.

Priority Actions

- Increase coordination with customer agencies to fully automate the process.

- As part of the FBI's information technology modernization efforts, upgrade the name check application to increase accuracy and speed.

IVF.3 Improve the processing and quality of FBI responses to FOIPA requests.

The FBI has made several process improvements to address the increasing public demand for FBI information. However, dramatic improvements can only be achieved through modernization of the FBI's information technology systems.

Priority Actions

- Develop a paperless FOIPA process including an Internet-based request and response capability.

- Ensure FOIPA processes are fully addressed in the FBI's future electronic record keeping system.