

8

Strategic Goal Eight: Ensure Professionalism, Excellence, Accountability and Integrity in the Management and Conduct of Department of Justice Activities and Programs

Strategic Objective & Annual Goal 8.1: Integrity And Professionalism Promote integrity and professionalism to ensure the fair and impartial administration of justice

8.1A Ensure Departmental Integrity

In order for its programs and activities to be effective, all Department personnel, contractors, and grantees must conduct themselves in accordance with the highest standards of integrity, accountability, and efficiency. The Office of the Inspector General (OIG) was established to detect and prevent misconduct and mismanagement on the part of the Department's personnel and programs. OIG investigates alleged violations of criminal and civil laws, regulations, and ethical standards arising from the conduct of the Department's employees in their numerous and diverse activities. OIG provides leadership and assists management in promoting integrity, economy, efficiency, and effectiveness within the Department and in its financial, contractual, and grant

relationships with others using the coordinated efforts of OIG's investigative, audit, and inspection resources.

Performance Measure: Investigations Closed [OIG]

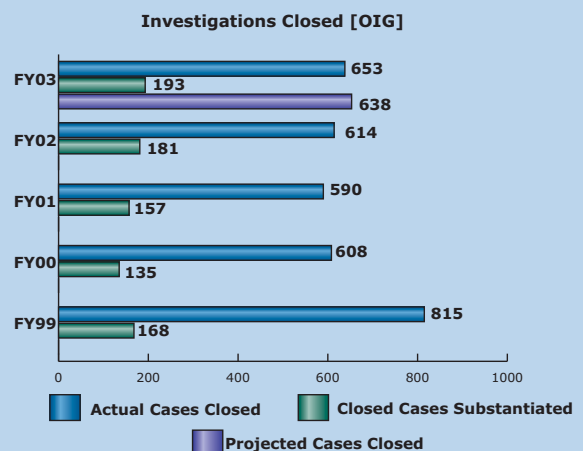
- **FY 2003 Target:** 653 Investigations Closed
- **FY 2003 Actual:** 638 Investigations Closed; 193 Closed Cases Substantiated
- **Discussion:** The OIG met 98% of its target. In FY 2003, approximately 5% of the investigative personnel resources were transferred to the newly created Department of Homeland Security's Office of the Inspector General.

Data Definition: Cases that are substantiated are considered to be those resulting in criminal or civil action, or referral to management for administrative action.

Data Collection and Storage: The OIG uses the Investigations Data Management System (IDMS) to collect data and track progress. IDMS consists of eight computer-based and four paper-based systems through which the Investigations Division records and monitors the status of allegations and the progress of investigations.

Data Validation and Verification: The Investigation Division is responsible for maintaining IDMS and ensuring accuracy and reliability through a semi-annual review of the information collected during that period.

Data Limitations: The IDMS lacks central indexing, which hampers data collection and analysis as the multiple systems require duplicate data entry and information is not cross referenced between systems. This can result in inaccurate or incomplete analysis. IDMS will be upgraded to eliminate these deficiencies in FY 2003. The upgraded IDMS II that eliminates these deficiencies will be operational in FY 2004.

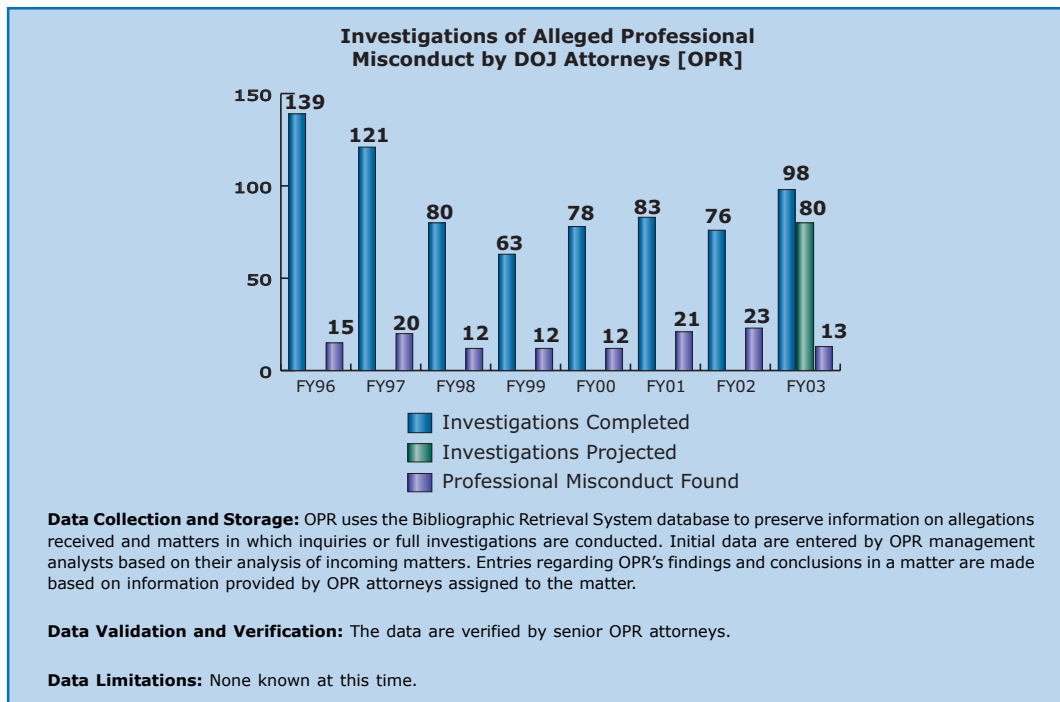


8.1B Provide Professional Oversight

The Department, through its Office of Professional Responsibility (OPR), ensures that Department attorneys meet and maintain the high ethical standards expected of the nation's principal law enforcement agency. Specifically, OPR reviews and investigates allegations of professional misconduct by Department of Justice attorneys, investigators or law enforcement personnel where the allegations relate to the exercise of an attorney's authority to investigate, litigate, or provide legal advice. Through the performance of OPR, the Department seeks to assure Congress, the courts, the state bars, and the public generally that Department attorneys, and investigative and law enforcement personnel working with the attorneys, comply with obligations and standards imposed by law, applicable rule of professional conduct, or Department regulations or policy, and that instances of failure to comply with those standards are identified, appropriate discipline is imposed, and the matters are referred to state bars.

Performance Measure: Investigations of Alleged Professional Misconduct by DOJ Attorneys [OPR]

- **FY 2003 Target:** 80 Investigations completed
- **FY 2003 Actual:** 98 Investigations completed
- **Discussion:** The number of investigations completed represents 123% of OPR's target. Thirteen were completed with findings of misconduct. A rigorous new case management process has increased productivity. It has permitted the assignment of resources in a more directly focused manner, thereby increasing the efficiency of the office. In conjunction with EOUSA, OPR has initiated a "Rapid Response Pilot Program" to develop the capability to respond to matters requiring expedited handling.



Strategic Objective & Annual Goal 8.2: Financial Management

Strengthen internal financial systems and promote the efficient and effective use of resources to ensure public trust and confidence

8.2A Obtain a Department-wide Unqualified Audit Opinion and Resolve Financial Management Weaknesses

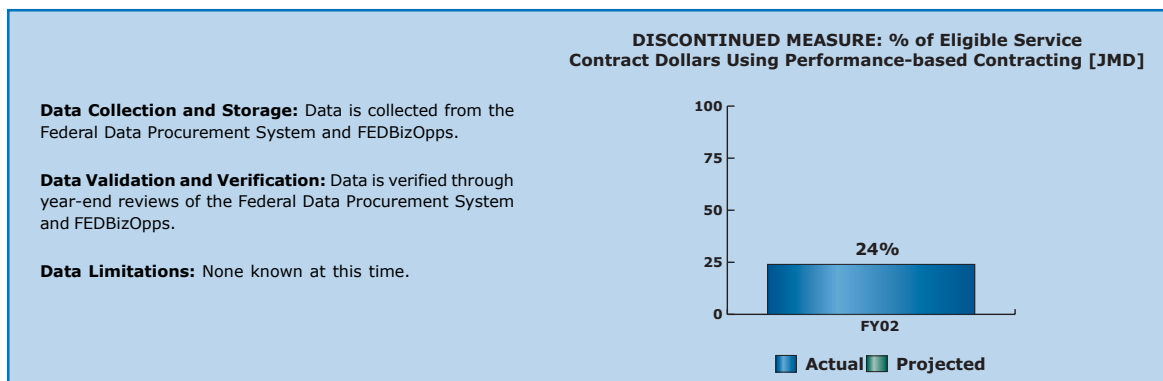
Full discussion of this topic has been moved to the PMA section on Improved Financial Management.

8.2B Achieve Procurement Reform

DOJ has been participating in two Government-wide procurement initiatives. The first, to encourage the use of performance-based contracts, was fully implemented in FY 2002. The second, the Central Contractor Registration database is an online database serving as the Government-wide single point of vendor registration. It is the single validated source data on vendors doing business with the Government.

Performance Measure: DISCONTINUED
MEASURE: Percent of Eligible Service Contract Dollars Using Performance-Based Contracting [JMD]

- **FY 2003 Target:** The OMB Office of Federal Procurement Policy re-evaluated performance based contracting in FY 2003. Therefore, there was not an established goal for FY 2003.
- **FY 2003 Actual:** See above.
- **Discussion:** Use of the Central Contractor Registration database was established in DOJ during FY 2003. Contracting Officials are assuring contractors are registered in the database and awards are made only to registered firms, except as appropriately authorized.



8.2C Conduct A-76 Program Competitions and Accurate FAIR Act Inventories

Full discussion of this topic has been moved to the PMA section on Competitive Sourcing.

8.2D Budget and Performance Integration

Full discussion of this topic has been moved to the PMA section on Budget and Performance Integration.

Strategic Objective & Annual Goal 8.3: Grant Management

Develop and maintain grant management accountability mechanisms to ensure proper dispensation and monitoring of funds

8.3A Achieve Effective Grant Management

Office of Justice Programs (OJP) and Community Oriented Policing Service (COPS) administer all grant programs for the Department of Justice. Full discussion of this topic has been moved to Strategic Goal Three.

Strategic Objective & Annual Goal 8.4: Information Technology

Improve the integrity and security of computer systems and make more effective use of information technology

8.4A Ensure IT Investments are Cost Effective and Meet Programmatic and Customer Needs

Under the direction of the DOJ Chief Information Officer (CIO), the Department provides leadership and policy direction to information technology (IT) programs in over 30 component organizations with widely divergent missions and funding. Cost-effective maintenance of current technology and timely adoption of new technology across the Department increasingly require coordinated management of technical, budgetary, and programmatic issues that impact IT investment.

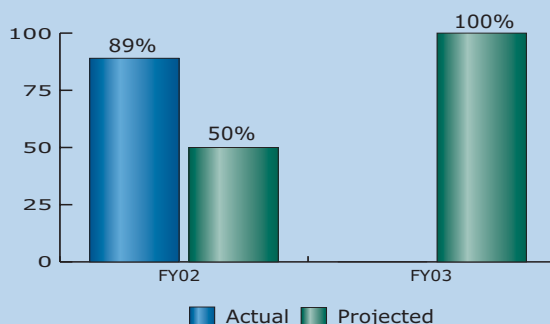
The Department has established a formal IT investment management (ITIM) policy and process to ensure that investment decisions are aligned with the strategic goals of the Department, are well-planned and justified, fit within the Department's overall IT strategy and enterprise architecture, and are managed effectively throughout the lifecycle.

Performance Measure: DISCONTINUED
MEASURE: DOJ IT Investments Managed Through the Approved ITIM (IT Management Investment) Process [JMD]

- **FY 2003 Target:** 100%
- **FY 2003 Actual:** 100%

- **Discussion:** In FY 2003, 2 remaining DOJ components (19 total) received approval from the CIO on their initial ITIM process and implementation schedules. ITIM allows the Office of the Chief Information Officer (OCIO) and the components to refocus information technology management to support the strategic missions of the Department. ITIM promotes an investment review process that drives budget formulation and execution for information systems, and rethinks and restructures the way DOJ performs functions *before* investing information technology to support that work. The Department continues to maximize the value of IT spending enterprise wide. This is evidenced by the consolidation of IT projects that represent an overall strategy consistent with CIO's strategic direction. Project consolidation efforts exist in enterprise infrastructure, enterprise architecture and financial management systems. Although we have achieved our actual target for this performance measure, OCIO will continue to focus on the application of information technology on improvement of DOJ mission performance, enhanced information security, reduced IT project duplication and continued coordination efforts enterprise wide in an integrated manner.

DISCONTINUED MEASURE: DOJ IT Investments Managed Through the Approved ITIM Processes [JMD]



Data Collection and Storage: Performance data for this indicator will be drawn from the A -11 Exhibit 300 B which is submitted to OMB annually as part of the budget.

Data Validation and Verification: Component and departmental managers reviews data.

Data Limitations: Potential comparability issues across components.

8.4B Ensure IT Security

Over the past several years, the Department has made the certification and accreditation of our information systems a priority. Systems approved in an earlier effort are now due to be reauthorized. IT systems and networks require formal authorization to operate every three years unless major changes or serious security problems require it more frequently. The Department continues to enhance its capability and tools used to track component security weaknesses and planned corrective actions identified through the certification and accreditation process and other security reviews, such as Office of the Inspector General audits and penetration tests. The Department's oversight and monitoring capabilities will include all the required functionality and performance measures for review, oversight, Federal Information Security Management Act (FISMA) reporting, and program and implementation management. Additionally, a major effort continues to gather, analyze, and enter data into an automated tracking tool for all systems not previously identified in earlier system assessments, update existing information on component systems, and input the results of various types of system and program reviews. This program is central to assuring the public's trust that information and IT systems in the Department are adequately protected against unauthorized access and use.

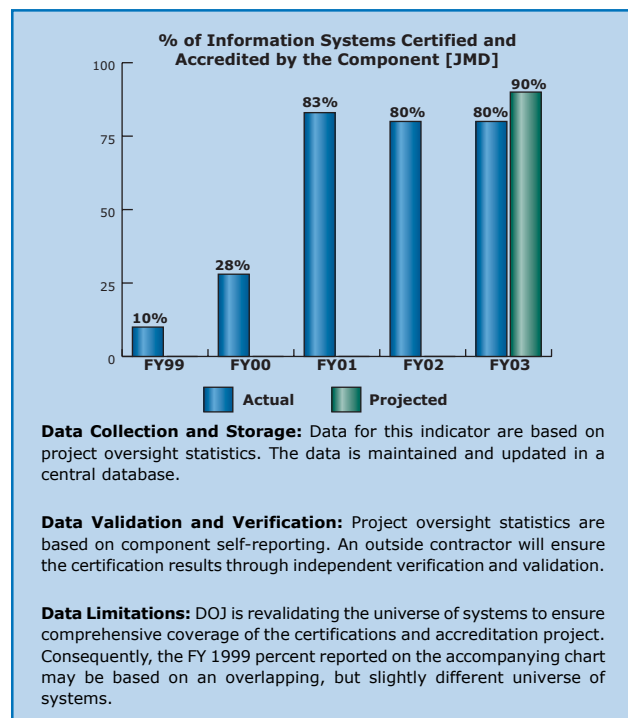
Performance Measure: Percent of Information Systems Certified and Accredited by the Component [JMD]

- **FY 2003 Target:** 90%
- **FY 2003 Actual:** 80% (202 of 253)
- **Discussion:** The Department employed several methods to conduct a more comprehensive and detailed review of its IT security program. To meet the FISMA requirements for annual system reviews and to identify vulnerabilities for correction, Department components conducted self-assessments on 163 systems in addition to assessments on 43 systems through new certifications and accreditations. A major change in the Department was the transferring of the Immigration and Naturalization Service (INS) to the Department of Homeland Security and the Bureau of Alcohol, Tobacco, and Firearms (ATF) to the Department. A high percentage of the INS' systems were accredited,

while a majority of the ATF's IT systems had Interim Approvals to Operate.

In the past year, the Department has made significant progress in meeting its objectives and implementing the requirements of the FISMA. These accomplishments include:

- Appointment of a deputy Chief Information Officer, heading a staff dedicated to the IT Security Program;
- Continuation of the effort to integrate security into the IT capital planning and budget processes;
- Continuation of the implementation and refinement of a Department system for tracking all IT security weaknesses and corrective actions;
- Continuing detailed planning activity for the Department's public key infrastructure initiative in a joint effort with the FBI;
- Developing an initial "to-be" IT security architecture; and
- Providing support to several large components for completion of risk assessment and certification and accreditation activities.

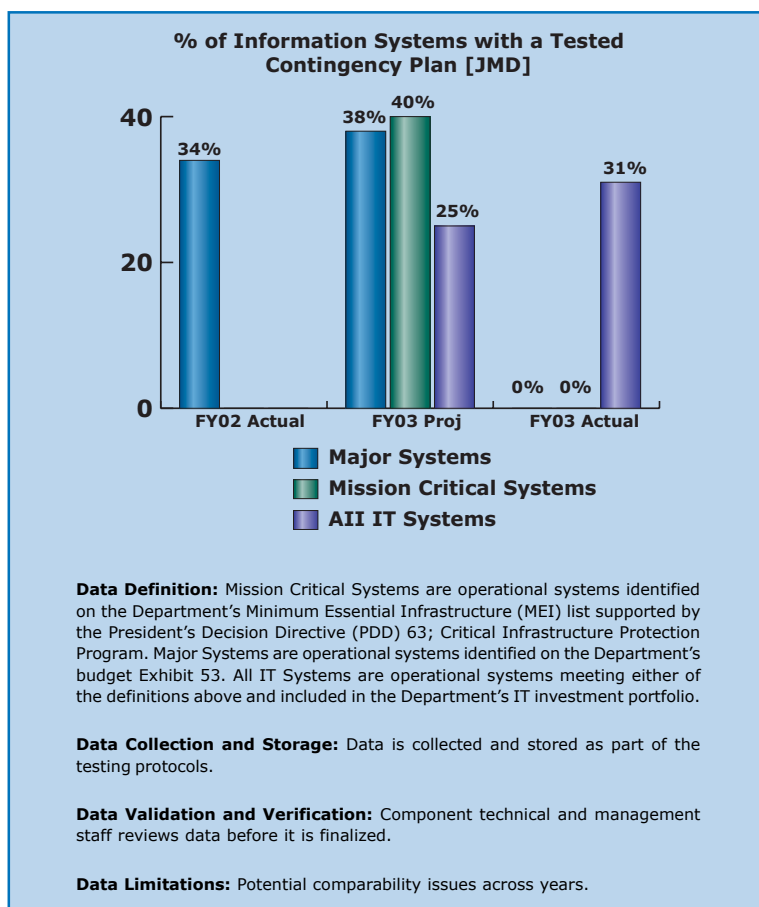


Performance Measure: Percent of Information Systems with a Tested Contingency Plan [JMD]

- **FY 2003 Target:** Critical 38% Major 40%, All Systems 25%
- **FY 2003 Actual:** N/A Critical; N/A Major; 31% All Systems
- **Discussion:** Although the Department conducted contingency tests as planned, certain components failed to track whether the system was “major” or “mission critical”. The initial reports generated to capture the data for this measure revealed additional common vulnerabilities in the Department’s systems related to tested contingency planning. The Department is taking steps to eliminate this

oversight in the future by adopting the National Institute of Standards and Technology (NIST) performance measures, tools and techniques to further strengthen our IT security program and show measurable progress.

The Department fell short of its percentage target even though the absolute number of major systems with tested contingency plans increased. As Department components integrate security life cycle activities and funding into the IT investment process, we expect these activities to be completed regularly for a higher percentage of our systems.

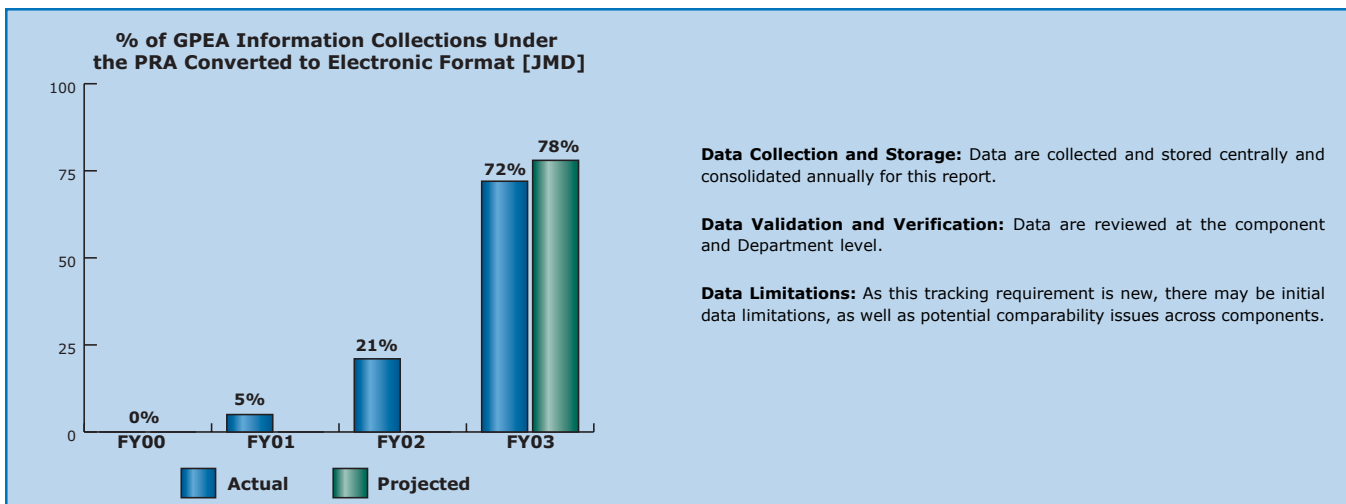


8.4C Expand Electronic Access and Dissemination of Department Information

The essence of the Government Paperwork Elimination Act (GPEA) is to provide citizens, businesses, and governmental agencies the option of conducting business with the Federal Government through electronic means. OMB considers that the information collections under the Paperwork Reduction Act (PRA) are the most significant transactions that should offer an electronic option as required by GPEA. Implicit within GPEA is transforming business processes to make them faster, more efficient, and more citizen-centric—key objectives of the “Expanded Electronic Government” initiatives in the President’s Management Agenda. Aggressive implementation of “eGovernment” initiatives is a priority of the Department’s IT Strategic Plan. The Department submitted the FY 2003 – FY 2004 eGovernment Implementation Plan to Office of Management and Budget (OMB) in October 2002.

Performance Measure: Percent of GPEA Information Collections Under the PRA Converted to Electronic Format [JMD]

- **FY 2003 Target:** 78%
- **FY 2003 Actual:** 72%
- **Discussion:** Although substantial progress was made in FY 2003, actual performance fell slightly short of the target. In several instances, projects were not completed in FY 2003 because components in the Department are seeking transformational changes in their capabilities by re-engineering their work processes and building infrastructure that will support secure, end-to-end processing of electronic transactions.



Strategic Objective & Annual Goal 8.5: Human Resources
Strengthen human resource recruitment, retention, and performance to ensure a workforce that is skilled, diverse, and committed to excellence

Full discussion of this topic has been moved to the PMA section on Strategic Management of Human Capital.

This page intentionally left blank.