

**Statement of
Dr. Paul R. Corts
Assistant Attorney General for Administration
U.S. Department of Justice
Before the
Committee on Government Reform
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
U.S. House of Representatives
March 16, 2004**

Mr. Chairman, Members of the Subcommittee:

I appreciate the opportunity to appear before you today to discuss the Department's efforts in the areas of information technology (IT) security and the efforts underway within the Department to institutionalize the daily management of information security risks and implement the requirements of the Federal Information Security Management Act. I would like to commend you and the Committee for your past and current efforts to shine the spotlight on Federal agency and security performance.

I wish to emphasize at the outset that the Department of Justice (DOJ) recognizes the importance of IT security and the Department's senior management is committed to fully protecting the Department's IT assets from attacks and vulnerabilities. I further wish to emphasize that responsibility for the Department's IT security program rests with the Department's Chief Information Officer (CIO).

Information technology (IT) is key to the Department's success in meeting our strategic goals. It provides new and improved capabilities to gather, analyze, and share intelligence information; identify, monitor, apprehend, and prosecute terrorist or criminal suspects; identify and prevent persons who are national security threats from entering the United States; securely share information with our federal, state, and local partners; efficiently manage our criminal and civil cases; provide accessible, speedy, and reliable services to our customers; and efficiently and effectively carry out our internal business practices. In addition, it provides the communications and computing infrastructure that ensures continuity of operations and rapid response in times of crisis.

The integrity and availability, and where appropriate the confidentiality and privacy of the information in our systems are today more important than ever. The value of computer and telecommunication systems and the vital information they process and transport became even more apparent in the wake of the tragic events of September 11th, 2001.

In the past, the Department operated in a very decentralized manner, and the IT computing environment and our IT security program was further fragmented within the Department. This has been a major concern with our Inspector General (IG) during the past years and has hampered mission accomplishment. Furthermore, we are fully aware of your concerns with our progress in information security and we take these concerns seriously.

Since I arrived at the Department of Justice 16 months ago, the Department has taken a number of actions that not only reflect the commitment of present management to correcting past deficiencies but also establish a solid foundation for sustained future progress. The accomplishments and initiatives we have underway address many of the IG's recommendations and will provide for improved performance in the coming year.

The current state of IT Security within the Department

The Department's IT security budget for FY 2004 comprises 3.7% of the planned IT portfolio of \$2,074 million. In FY 2003, we reported 253 IT systems, 24 programs, and 35 contractor operations and facilities. All of our programs and 206 (81%) systems were reviewed in accordance with the FISMA guidance provided by OMB and the National Institute of Standards and Technology (NIST). The Department incorporates IT security requirements in all of our contracts and further reviewed half of the contractor operations and facilities during the fiscal year. In addition, over 90% of our IT systems have been assessed for risks and over 80% have been fully certified and accredited to date.

In FY 2003, the Department implemented a web based computer security awareness training tool, to provide all employees and contractor personnel with access to Department systems basic end-user security training. During the first nine months of operation, we trained 77% of our employees and we stand committed to ensuring all employees and contractors receive basic security awareness training and that privileged users, such as system and network administrators and security professionals, receive specialized training.

The Department operates a computer emergency response team and has developed standards for reporting incidents within the Department. This group serves as the single point of contact to FedCIRC and verifies patch implementation at components. We are also working with the Department of Homeland Security to utilize their Project Matrix methodology to ensure the proper identification of our mission and national critical operations and assets. We are further committed to ensuring all of our systems have contingency plans in place and that these plans are tested at least annually.

Our CIO reports directly to the Attorney General for his duties and responsibilities identified by the Clinger-Cohen Act. Our CIO also serves as the Deputy Assistant Attorney General for Information Resources Management and is a vital part of our Departmental management team, and routinely coordinates IT initiatives and

programs through my office and with me as the Chief Financial Officer and the Procurement Executive.

Through the Attorney General's leadership and vision, we have come a long way toward a more centrally coordinated Department, and this has made a very positive impact on our total IT efforts.

In June of 2003, the CIO established an IT Security Office to oversee the implementation of the Department's IT Security Program, led by the chief information security officer. In November 2003, I signed a Departmental Order clarifying the CIO authority and responsibilities for IT security. This single point of authority for information security program management and oversight implements the IG's recommendation to provide a central IT security office. This office is responsible for developing IT security policy and standards, and has organized a security council comprised of top security officials from each of the Department's component organizations. In addition, our IT Security Office coordinates with other security programs, including personnel and physical security.

The Department has integrated IT security within the capital investment process and the system development life cycle. We are continuing to develop a security architecture as an integrated element of our enterprise architecture, so that the IT investment process and our future infrastructures adequately incorporate our security needs and prevent IT security failures in the future.

In addition to the strategic improvements identified above, we have been addressing many of our known weaknesses within our current operations through our curative efforts. These efforts include certifying and accrediting our legacy systems, identifying vulnerabilities and weaknesses through regular risks assessments and testing of security controls. In addition, we have been implementing near term fixes and monitoring corrective plans of actions and milestones (POA&Ms) to provide for an overall net reduction in risk.

In our FY 2003 Accountability Report, we reported two material weaknesses relating to IT security, one of which is a Department level material weakness relating to component implementation of management, operational, and technical security controls and the other is specific to securing the FBI's infrastructure and implementing an IT security program. Both material weaknesses are from the previous year and have associated plans of actions and milestones to manage corrective action.

Actions underway to remedy deficiencies in IT security reported in FISMA and financial reporting

IT security is a high priority within our Department. Accountability and responsibility is critical to our successful remediation of identified vulnerabilities and weaknesses. The Department's senior management team is committed to ensuring

activities are underway and planned to correct past deficiencies and to ensure future practices are institutionalized.

In addition to the many strategic initiatives identified previously, we have identified additional initiatives to further address the program and system level weaknesses identified in our FISMA and financial management reporting. At the program level we have:

- Developed a Department-wide IT Security Program to assess and reduce risk;
- Established IT security program goals;
- Identified program level resources;
- Approved policy and 17 information security standards for management, operational, and technical control requirements;
- Chartered an IT Security Council and six project teams to manage implementation and assist operational managers;
- Developed a Department-wide information security training and awareness program; and
- Implemented a monthly report card for monitoring component progress.

And at the system level we have:

- Integrated IT security with the enterprise architecture and investment management processes;
- Scheduled to achieve full approval to operate for 90% of all IT systems by July 2004;
- Developed system risk assessment and test plan tool incorporating over 250 management, operational and technical risk control requirements;
- Scheduled periodic validation testing to be completed by July 2004; and
- Developed a process for planning, resourcing, implementing and maintaining risk control requirements.

Additionally we have:

- Provided for CIO collaboration and review of Component corrective action plans;
- Implemented an initial capability for an integrated Department-wide tool used for documenting and evaluating system security controls and risk management and monitoring program and system corrective POA&Ms;
- Continued development of a public key infrastructure capability to support enhanced authentication controls and strategic initiatives in information sharing;
- Continued development of a unified financial management system across the Department that will incorporate the financial management and security practices; and
- Provided additional oversight and resources to assist troubled components in assessing their systems, developing POA&Ms, and ensuring development of certification and accreditation documentation.

Institutionalizing Information Security within the Department

As I previously stated, we have created a solid foundation for future implementation and effective management of information security across our Department. In July 2002, we issued the Department's Information Technology Strategic Plan. The plan, approved by the Department's Strategic Management Council (SMC), represents a starting point for what will be a long-term, sustained, and collaborative effort to significantly improve IT in our Department. We are focusing on four key areas: 1) IT infrastructure, 2) information security, 3) common solutions, and 4) management roles and processes. These four areas have been chosen because, together, they represent the core building blocks of the Department's IT program. Progress in implementing the IT Strategic Plan is monitored by my office in conjunction with the Strategic Management Council, on behalf of the Attorney General. Key management positions in the Office of the CIO are now filled with staff from the Senior Executive Service to lead the new organization in support of the Attorney General and the President's Management Agenda. The CIO continues to build the organizational capacity to carry out this ambitious mission as the new organization is implemented to support our IT strategy and operations.

I am pleased that we have been able to implement reorganization of our Department level IT organization. Among the main objectives of this reorganization was the elevation of the role of IT security, the enforcement of the importance of IT security, and the clarification of lines of responsibility and accountability. The reorganized Office of the CIO includes a senior information security official and establishes an IT security staff reporting directly to the Department's CIO. This staff is responsible for ensuring that all component systems have implemented the appropriate IT security controls, for ensuring that components identify POA&Ms when the security controls are not met, and for monitoring these corrective action plans. The new organization for the Office of the CIO was approved by the Attorney General, reviewed by the Office of Management and Budget (OMB) and the Congress, and implemented in May 2003.

The Department CIO has been working closely with component CIOs to ensure that program roles and responsibilities are defined and implemented. We are continuing to enhance and extend the use of standards and automated tools to help assess security controls and prioritize and monitor the implementation of corrective actions and to incorporate all known agency security weaknesses. We also are increasing our independent validation and monitoring of compliance with Departmental policy and practices, and ensuring that costs for security are identified in IT capital plans. At the same time, we continue to explore Department-wide infrastructure solutions that incorporate security and address crosscutting problems. For example, the Department is in the process of implementing a common telecommunications network that implements the security architecture for the wide area network and integrates many of the common security controls for the local computing environments.

We are also aggressively recruiting qualified IT security professionals to support system implementation and validation of security controls within our systems. We are

utilizing several unique government programs to strengthen our staff, which now includes direct hire authority for IT Security Professionals, and recruitment of Cyber Corps graduates and Presidential Management Fellows.

Furthermore, our Chief Information Security Officer has established a solid foundation for component integration with standards and procedures. We have implemented a monthly report card for each component to monitor performance. An example of the report card is summarized in the attached chart. Our overall objective is for our components to be green in each category and achieve full approval to operate on over 90% of our systems by October 2004.

The accomplishments and initiatives we have underway address many of the IG recommendations and will provide for improved performance in the coming year. We do acknowledge the need to demonstrate continuous improvement in our IT security program, while at the same time reduce the net risk associated with our IT assets.

I want to thank you and the Subcommittee for your continued focus on this important area. I would be pleased to take any questions at this time.