

Outcome Goal IT – Provide Improved, Secure IT Service to Citizens, Businesses, Government, and DOL Employees to Improve Mission Performance

Effective management of information technology is critical to the success of nearly every facet of DOL's programs and operations and corresponds to the E-Government initiative of the President's Management Agenda. DOL strives to use information technology to deliver better service to citizens, businesses, other governments, our federal partners and employees. To meet our goals, we are implementing a comprehensive, integrated E-Government framework, taking full advantage of the rapidly changing technological environment and to adapt to changes brought forth by the digital economy.

DOL is a recognized leader in integrating IT capital planning and enterprise architecture activities with broader Federal and Departmental priorities. This integrated approach to managing our information technology portfolio enables us to identify future environments and to ensure IT remains closely aligned with our mission, goals, and objectives. DOL will continue to lead the GovBenefits Presidential Priority Initiative and participate actively in implementing the Federal E-Government Strategy by partnering with other agencies.

Goal (Agency) – Period Goal Statement [Achievement]	Performance Summary
IT1 (OASAM) – FY 2004 E-Government – Utilizing Technology to Improve Service and Efficiency [Not Achieved]	The system was implemented in both the National and Regional Offices for 14 DOL component agencies. Substantial progress was also achieved toward the interface with GSA Advantage. Final testing is underway for on-line shopping, which will be available by the end of September 2004. DOL did not reach its GPEA target of automating 100 percent of designated manual processes.
IT2 (OASAM) – FY 2004 Improve the performance of the Department's Cyber Security Program in accordance with the Federal Information Security Management Act (FISMA). [Achieved]	The Department reached its Cyber Security Program indicator targets, exceeding projections regarding System Tests and Evaluations and internal Computer Security Incident Response Reporting.
IT3 (OASAM) – FY 2004 Improve organizational performance and effective information management through the use of the Departmental IT Capital Planning Investment Control process. [Achieved]	All targets were reached. Rollout and migration of the Department's new tool for electronic capital planning and investment management was achieved. Agencies used the tool to prepare their FY 2006 IT budget submissions. DOL reached its target of initiatives operating within 10 percent of cost, schedule, and technical performance parameters. DOL also reached its target for 95 percent of major IT initiatives completed during FY 2004 to deliver intended benefits.

Results Summary

IT Goals 2 and 3 were achieved, while IT Goal 1 was not achieved. We continue to plan, acquire, and implement new information technology, business solutions, services and capabilities. Our now-operational web-based e-procurement system (EPS) provides a comprehensive toolset for extended acquisition capabilities. It takes advantage of technological advances in order to streamline processes, improve customer service, and reduce costs. Additionally, EPS provides more reliable and accurate department-wide procurement-related financial information. Internal factors impacting the implementation include interfaces with the new DOL property system. The Department's Directory Service will automate data reconciliation and make information in existing directories accessible and re-useable even when the database formats differ. The design calls for the implementation of a metadirectory capable of pulling data from and distributing it to multiple directories based on defined business rules. This capability, after integration into the department's myriad systems, will eliminate mismatches caused when similar information is manually entered into multiple databases. A metadirectory should also eliminate redundant work in maintaining DOL's various electronic directories.

Future Challenges

DOL continues to plan, acquire, and implement new information technology, business solutions, services and capabilities, and will soon fully implement an Earned Value Management System to better manage IT projects while in development.

Make DOL an E-Government Model

Performance Goal IT1 (OASAM) – FY 2004

E-Government - Utilize Technology to Improve Service and Efficiency

Indicators

Automate 100 percent of the manual processes designated under GPEA;

Implement the web-based e-procurement system (EPS) to seven DOL component agencies; and

Establish an Enterprise-wide Directory Service.

Program Perspective

The web-based e-procurement system (EPS) provides a comprehensive toolset for extended acquisition capabilities, by taking advantage of technological advances in order to streamline processes, improve customer service, and reduce costs. EPS provides more reliable and accurate department-wide procurement-related financial information. The Department's Directory Service will automate data reconciliation and make information in existing directories accessible and re-useable even when database formats differ. The design calls for the implementation of a metadirectory capable of pulling data from and distributing to multiple directories based on defined business rules. This will eliminate mismatches caused by manual data entry into multiple databases, and alleviate directory administration burdens.

Results, Analysis and Future Plans

This goal was not achieved. DOL reached the web-based (EPS) target, and the system was implemented in both the National and Regional Offices in 14 DOL component agencies; the target was for implementation in seven agencies. DOL also completed interfacing EPS with 'GSA Advantage'. Our target to establish an enterprise-wide directory services was reached. The directory service, with Windows 2003 Active Directory as its foundation, has moved from its interim design in April 2003 to the target design. This phase of the initiative is fully compliant with the Department's System Development Life Cycle Management, and received its Authority to Operate (ATO) from the Department's Chief Information Security Officer in July 2004. Achieving this indicator simplifies and unifies DOL's many directory functions, including email services. Our GPEA indicator remained at mid-year status of 93 percent, failing to reach the 100 percent target.

Performance Goal IT1 (OASAM)			
E-Government – Utilizing Technology to Improve Service and Efficiency			
	Result	Target	*
Automate 100% of the Designated GPEA Manual Processes.	93 %	100%	N
Implement Web-based EPS in seven DOL component agencies.	14	7	Y
Establish an Enterprise-wide Directory Service (EDWS).	Y	Y	Y

*Indicator target reached = (Y), substantially reached = (S) or not reached (N)

Management Issues

Performance data for this performance goal is based on internal tracking activities for progress on E-Government initiatives, E-Procurement Implementation, and E-Government Workforce efforts. DOL monitors these activities and produces quarterly progress reports. Internal factors impacting the implementation of the EPS include interfaces with the new DOL property system. Also, management will need to focus on interfacing the new property system and EPS with the new financial system. The complexity of the interface and its ability to enable some of the EPS functionality will drive the costs and timing.

Make DOL an E-Government Model

Performance Goal IT2 (OASAM) – FY 2004

Improve the performance of Department's Cyber Security Program in accordance with the Federal Information Security Management Act (FISMA).

Indicators

Ensure that 95 percent of DOL's sensitive systems have been periodically assessed for risk and magnitude of harm that might result from unauthorized access;

Ensure that at least 60 percent of all weaknesses documented in the FY 2004 POA&Ms are closed or on schedule;

Ensure that at least 90 percent of all DOL sensitive systems are fully certified and accredited during FY04;

Ensure that at least 98 percent of all DOL employees and contractors receive annual security awareness training;

Ensure that System Test and Evaluation has been conducted on at least 85 percent of DOL's sensitive systems;

Ensure that at least 50 percent of DOL agencies respond to DOLCSIRC advisories in accordance with the procedures in the DOL Computer Security Handbook;

Ensure that at least 95 percent of all DOL sensitive systems have contingency plans; and

Ensure that at least 50 percent of the contingency plans have been tested.

Program Perspective

The Department is faced with the increasingly difficult challenge of protecting its automated information resources given the ever-increasing number of IT security threats. DOL's Cyber Security Program's purpose is to identify and afford security protections. These protections are commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of information collected or maintained by the Department. Protecting the Department's critical IT resources requires the adoption of reasonable precautions for securing its systems and networks. It also requires quick and effective response if system and network security defenses are breached. To that end, the Department's Cyber Security Program must be one that is comprehensive and inclusive of internal policies and guidelines that ensure the integrity, availability, confidentiality and security of its operations and assets.

In providing the protections mentioned above, the Cyber Security Program must provide an effective means for measuring and enhancing its information security program performance and must ensure its compliance with the Federal Information Systems Management Act (FISMA).

Results, Analysis and Future Plans

DOL achieved its Cyber Security Program performance goal. DOL will reach targets for system tests and evaluations and for internal computer security incident response reporting.

Performance Goal IT2 (OASAM)			
Improve the performance of Department's Cyber Security Program in accordance with the Federal Information Security Management Act (FISMA)			
	Result	Target	*
1. Percent of DOL's sensitive systems that have been periodically assessed for risk and magnitude of harm that might result from unauthorized access.	95%	95%	Y
2. Percent of all weaknesses documented in the FY 2004 Plan of Actions and Milestones (POA&Ms) closed or on schedule.	65%	60%	Y
3. Percent of all DOL sensitive systems fully certified and accredited during FY 2004.	94%	90%	Y

Performance Goal IT2 (OASAM)				
Improve the performance of Department's Cyber Security Program in accordance with the Federal Information Security Management Act (FISMA)				
4.	Percent of all DOL employees and contractors that receive annual security awareness training.	98%	98%	Y
5.	Percent of DOL's sensitive systems for which a System Test and Evaluation was conducted.	94%	85%	Y
6.	Percent of DOL agencies that respond to Computer Security Incident Response Capability (DOLCSIRC) advisories in accordance with the procedures in the DOL Computer Security Handbook.	60%	50%	Y
7.	Percent of all DOL sensitive systems with contingency plans.	98%	95%	Y
8.	Percent of contingency plans tested.	52%	50%	Y

*Indicator target reached = (Y), substantially reached = (S) or not reached (N)

DOL has continually improved the performance of its Cyber Security Program. According to the Federal Computer Security Report Card issued by Congress, the Cyber Security Program has progressed from a grade of "F" in 2000 and 2001, to a grade of "C+" in 2002. The current grade (assessed in 2003) is a "B."

Indicator three, relating to certification and accreditation, has the greatest importance to the achievement of greater IT security. Certifying and accrediting major information systems gives the Department a level of assurance that the Cyber Security Program is operating effectively. There are no planned changes to the goals or indicators for FY 2005. However, because IT security is crucial, targets for each of the indicators will be more ambitious.

The Security program is integrated into all Departmental program areas such as the Enterprise Architecture, Capital Planning and Investment Control, the System Development Lifecycle, and our strategic plan. The Department is committed to its Computer Security Program, and will continue to ensure that resources are adequately allocated for the proper protection of our information systems.

Management Issues

OIG identified three reportable conditions related to IT security:

1. The Department lacks strong logical security controls to secure the Department's data and information;
2. The Department has not developed and performed comprehensive tests of all continuity of operations/disaster recovery plans for critical systems and processes; and
3. The Department has not corrected all known vulnerabilities associated with its systems.

The Office of the Chief Information Officer (OCIO) has completed several actions to mitigate the vulnerabilities associated with these reportable conditions. These actions include, but are not limited to:

1. Advising senior management to give priority attention and resources to their agency specific conditions;
2. Establishing focus group to leverage agency expertise to develop action plans to address the systemic issues;
3. Performing a comprehensive review of applicable Departmental policies and procedures; and
4. Making necessary revisions.

The performance data used by the OCIO Security team is reliable and complete. The metrics used are those required by OMB. Performance data is gathered on a quarterly basis from DOL agencies and is validated by the OCIO Security team via internal verification and validation processes, quarterly Capital Planning and Investment Control reviews, and e-Government reviews. The OCIO Security team also performs reviews of its own internal processes and procedures to ensure the efficiency and effectiveness of the Department's Cyber Security Program, thus ensuring the completeness of the performance data.

DOL has made considerable progress on all reportable conditions. The only risk to achieving its goal is the lack of funding for comprehensively testing contingency plans. The OCIO has guided DOL agencies to approach this requirement by developing incremental test plans, which allow economical testing.

For more information on these audits, see Study 8 in Appendix 2.

Sound IT Capital Planning

Performance Goal IT3 (OASAM) – FY 2004

Improve organizational performance and effective information management through the use of the Departmental IT Capital Planning Investment Control process.

Indicators

95 percent of major IT initiatives completed during FY 2004 deliver intended benefits;

87 percent of in-process IT initiatives evaluated operate within 10 percent cost, schedule, and technical performance parameters; and

Rollout and migration to new investment management application for use during the FY 2006 budget cycle.

Program Perspective

The Clinger-Cohen Act requires agencies to use a disciplined capital planning and investment control process to acquire, use, maintain, and dispose of information technology. The Act seeks to improve performance by requiring agencies to clearly define and implement an IT Capital Planning and Investment Control (CPIC) process. This process is comprised of three distinct phases: select, control, and evaluate. The purpose of the CPIC process is to ensure that each IT investment aligns with DOL missions and supports business needs, while minimizing risks and maximizing returns throughout the investment's life cycle. It also allows decision-makers to make prudent evaluations of an investment's costs, benefits, risks and support for the DOL strategic goals and objectives when compared to other competing IT requirements.

In FY 2004, DOL established policy for, and implemented an earned value management system (EVMS) for major IT investments. EVMS routinely captures standardized, detailed information for monitoring cost, schedule and performance of major IT investments over time. By keeping track of this data in a systematic fashion, project managers and DOL management receive timely progress information on IT development projects. DOL management is also able to make informed decisions about projects' direction and the merits of continued investment in specific IT projects. DOL's EVMS is compliant with current standards and guidance from the Office of Management and Budget.

Results, Analysis and Future Plans

This goal was achieved. All targets were reached. Rollout and migration of the Department's new tool for electronic capital planning and investment management was achieved in the 2nd quarter FY 2004. Agencies used the tool to prepare their FY 2006 IT budget submissions. At 93 percent, DOL exceeded the 87 percent target for initiatives operating within ten percent cost, schedule, and technical performance parameters. DOL also reached its target for 95 percent of major IT initiatives completed during FY 2004 delivering intended benefits.

DOL is committed to ensuring that information technology investments are based upon decision criteria that considers risk-adjusted return, emphasizes interoperability, improves delivery of services, and reduces costs. Achieving this goal is key to the success of the capital investment management process. Employing the Electronic Capital Planning and Investment Control (eCPIC) system facilitated the management of Department-wide IT investments and the preparation of budget data for submission to OMB. In addition, the rollout of EVMS produces monthly project data and shows trends over time. DOL will continue to develop goals and indicators, and set targets designed to ensure compliance with the IT Capital Investment Management Process; and support and assist agency managers and analysts in executing the IT capital investment management process through guidance, training, and oversight.

Management Issues

To ensure the reliability of performance data and to ensure that project outcome goals are positively achieved with the cost, schedule, and performance projections, DOL uses a combination of performance-based management mechanisms, including the earned value management system and a quarterly review process. Work Breakdown Structures (WBS) are required and updates are provided to the OCIO upon request. Actual start and completion dates, percentages complete and estimated costs are assessed against each element in the WBS. Based on the information provided, an investment's performance is assessed, and cost and schedule variances are calculated.

To mitigate the risk to project performance, cost and schedule variances are reported to senior management within the Department, and mechanisms have been put in place for addressing projects which exhibit poor performance. Such projects are closely reviewed during periodic reviews with the project manager, and corrective actions are developed and assigned. Progress of corrective actions is frequently checked to ensure that the project is on track.