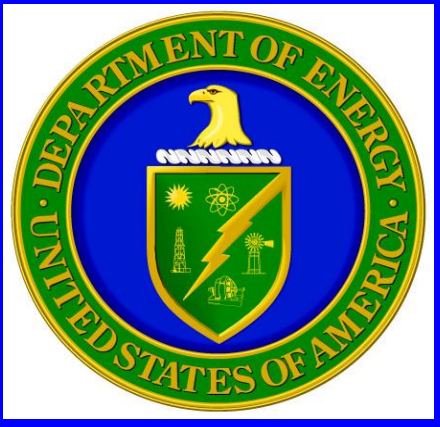


U.S. Department of Energy

INFORMATION TECHNOLOGY CAPITAL PLAN

September 2008

Office of the Chief Information Officer

TABLE OF CONTENTS

INTRODUCTION

In accordance with the Clinger-Cohen Act, Office of Management and Budget (OMB) Circular A-11, and OMB Circular A-130, this is the annual submission of the Department of Energy's (DOE) Information Technology (IT) Capital Plan (the Plan) that accompanies the Department's 2010 budget submission. This Plan describes existing DOE IT capital planning processes, the future strategy for managing IT investments efficiently and effectively through an Agency-wide risk-based security program, and describes the Departmental Enterprise Architecture (EA) and Security approaches. This Plan presents the steps DOE is taking to improve its Capital Planning and Investment Control (CPIC) processes, which have been documented in the Department's CPIC Process Guide, September 2008. The CPIC Process Guide includes a description of the IT governance process and the end products, such as the DOE IT Portfolio (Exhibit 53) and Exhibit 300s. The Guide also details the Select, Control, and Evaluate phases of the CPIC process and the integration of the CPIC processes with other IT investment management components at the Department.

Consistent with the requirements identified in OMB Circular A-130, this Plan contains the following sections.

- **Section 1:** A description of the existing IT investment management and governance processes
- **Section 2:** Lessons learned from the existing processes
- **Section 3:** A summary of the DOE EA
- **Section 4:** A summary of the DOE cyber security program
- **Section 5:** A summary of the DOE IT reports submitted with the budget
- **Appendix A:** DOE's self-scoring of the budget year (BY) 2010 Exhibit 300s

1.0 EXISTING INVESTMENT MANAGEMENT GOVERNANCE AND PROCESSES

1.1 BACKGROUND

DOE manages its information technology assets through IT governance processes. IT governance is the Department's basic mechanism for analyzing and making IT decisions through a lean management structure that has the appropriate degree of authority and division of responsibilities. During fiscal year (FY) 2008, the Department's IT Council (ITC) continued to support the Chief Information Officer (CIO) in helping to coordinate IT management within the DOE. The main priorities of the ITC are to promote collaboration and the effective and efficient acquisition and use of information resources, work to reduce the cost of operations, and improve the management and execution of the Department's IT investments in achieving DOE's mission. The ITC is composed of the senior IT managers from all of the DOE program and support offices. It also includes ad-hoc groups with specific roles in support of Council management functions, including the Consolidated Infrastructure Integrated Project Team (IPT) to support the management of the Department's infrastructure and advisory board members from the Nuclear Weapons Council (NWC), the Energy Facility Contractors Group (EFCOG), and the Systems of Labs' Computing Coordinating Committee (SLCCC) leadership.

The current DOE governance process builds upon several key activities that have been in place at DOE for some time. These activities are discussed below.

A major focus of DOE's governance improvement process is based upon DOE Order 413.3 (Order 413). This order addresses the requirements for managing the acquisition of capital assets, initiation through implementation, and describes the associated decision points, decision-makers, and documentation results throughout the process. In FY 2008, the OCIO and the Office of Engineering and Construction Management (OECM) continued the development of an IT Project Guide for the Order to provide federal project directors, the IT project managers, integrated project teams, program managers, program offices, and acquisition executives with additional guidance on complying with Order 413 requirements. The guide addresses the acquisition of IT capital assets and the management of IT projects and programs.

A key tenet of Order 413 is a signed memorandum which requires program offices to report IT project status in the Project Assessment and Reporting System (PARS) to provide for better managerial oversight. Any investment of $5 million or greater Total Project Cost (TPC) will be required to report monthly project status through PARS. TPC is defined by Order 413 to be the total of planning and acquisition costs for a project. For IT investments, this equates to the development, modernization, and enhancement (DME) costs. IT investments less than $5 million TPC will remain under program office control and oversight. In addition to the mandatory thresholds cited above, the OCIO reserves the right to require any investment in the DOE IT portfolio to regularly report as deemed necessary. Finally, all investments in the portfolio will be reviewed annually through the integrated DOE capital planning and budget processes. This layered approach to IT reporting, oversight and management will ensure that all IT investments are reviewed and managed commensurate with their risk and criticality.

Another key focus of DOE's IT investment management process is the delivery of results. DOE policy dictates the use of earned value management (EVM) for all major IT investments with total lifecycle DME costs of $20 million and above and DME costs that exceed $5 million in the current (CY) or budget year (BY). In June 2006, the

responsibility for EVM oversight was transferred from the OCIO to the Office of Engineering and Construction Management (OECM), as stated in a signed memorandum dated June 29, 2006. The OCIO and OECM continue to work together in ensuring the oversight and the management of the Department's IT projects while remaining in accordance with regulatory oversight such as the Clinger-Cohen Act.

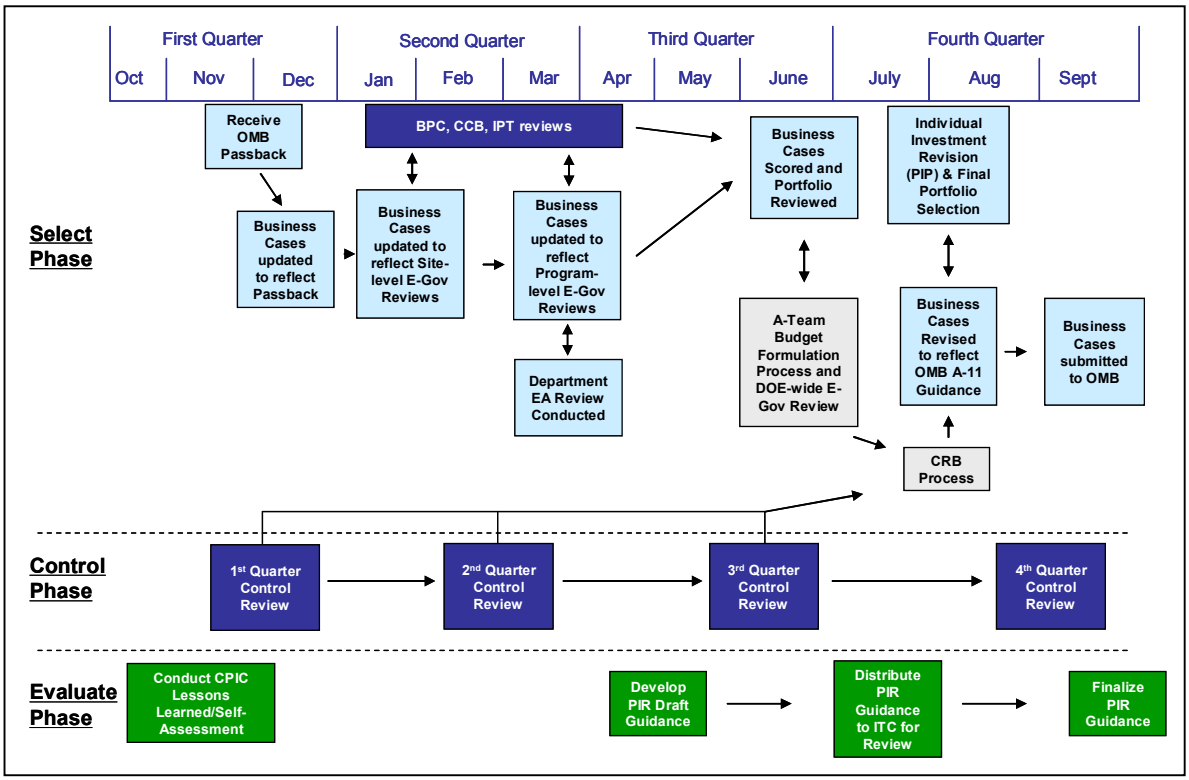
During FY 2008, the OCIO also refined its EVM guidance to program and support offices. Project managers were asked to provide additional details of the cost of full-time equivalents in their cost and schedule milestones during development and operations. Also, project managers were asked to provide additional information on DME milestones and EVM Systems. IT governance for EVM was re-emphasized by having project managers continually update the IT Council regarding investments with corrective actions for cost or schedule variances that exceed + or – 10%. In addition, operational metrics used in Control Reviews were aligned with the ANSI/EIA-748 EVMS Standard.

In FY 2008, the Office of the CIO (OCIO) also continued to update DOE Order 200.1, Information Technology Management, which provides an overall framework for managing IT resources throughout the Department. The update ensures that the Order is fully aligned with all current DOE policies, orders, and processes.

1.2 PROCESS DESCRIPTION

IT CPIC at DOE involves three phases as described below – Select, Control, and Evaluate. The Select phase has a dual focus: selecting new investments into the IT portfolio, and selecting existing investments into particular reporting portions of the IT portfolio each year. The Control phase focuses on the performance of all major investments on a quarterly basis. The Evaluate phase focuses on investments (or portions of investments) that have been fielded and are in the operations and maintenance (O&M) life-cycle phase. These three phases focus on various investments based on the budget cycle and the investments' life-cycle stage and are all conducted across the course of the year. The figure below shows the primary activities associated with each stage, across the typical budget year.

Figure 1: DOE Annual Roadmap



1.2.1 Select Component

1.2.1.1 Select Process Description

The Select phase encompasses screening, scoring, and selecting investments that support the DOE EA and modernization blueprint and meet the requirements of OMB Circulars A-11 and A-130, and DOE Order 413. The process steps are as follows:

- Screening
  - The program and staff offices define requirements; evaluate the target performance outcomes and business processes needed to meet those requirements; determine the IT applications and infrastructure required; review all proposed investments to ensure that investments align with key priorities; analyze duplicative investments to determine if they can be phased out; and develop the IT portfolio consistent with the program budget submission.
  - As new requirements are identified, the program and staff offices submit a Mission Need Statement in accordance with Order 413. As the requirement is approved and passes through various planning stages, it follows specific critical decision points, where designated senior management (the Acquisition Executive for a particular capital asset), approves Order 413-specified steps, documents, plans, and activities. The Acquisition Executive is supported in this process, as required, by an advisory board (equivalent to the Energy System Acquisition Advisory Board for major system projects) including program office, the Office of the Chief Financial Officer (OCFO), and OCIO representatives.

- Annually, all of the approved requirements are captured in the proposed IT portfolios from the program offices, are forwarded to the CIO and CFO with budget request data, and are incorporated into the DOE-wide IT portfolio. Select information is provided to the OCIO in the form of OMB Exhibit 300 business cases, other budget request documentation, and program office submissions to the Department's OMB Exhibit 53. All Exhibit 53 entries and Exhibit 300s are maintained, updated and submitted using the eCPIC application. This allows the Department to maintain a repository of all investment information.
- These program office IT portfolios are merged with staff office IT portfolios to create the Department's proposed IT portfolio.

- Scoring
  - The OCIO reviews, scores, and develops a performance improvement plan (PIP) for each major IT investment business case. The OCIO uses an integrated project team (IPT) of representatives from the IT Capital Planning and Architecture Division and the offices responsible for E-Government, Cyber Security, Privacy, and Records Management to perform the internal review.
- Selection
  - The program and staff offices then update their respective business cases by addressing the items in the PIP and submit a final business case to the OCIO.
  - This review and revision process is repeated until a final business case is accepted by the OCIO as a valid, viable business case.
  - The ITC then votes on the portfolio in late August and provides final, Agency-level approval of the BY 2010 requests for major IT investments.

1.2.1.2 Select Phase and the Budget Process

The OCIO works closely with the OCFO throughout the budget season to ensure the Select phase is fully integrated with the Department's larger budget preparation process. The DOE Analysis Team (A Team) provides analysis and recommendations to the Corporate Review Budget (CRB) Board on IT investments, as well as other budgetary items. An IT representative serves on the A Team to ensure that IT issues are adequately addressed. The CRB is the second phase in the annual budget formulation process responsible for determining the Department's budget submission. The CRB seeks input on IT investments from the A Team, CIO and the CFO. The CRB Board reviews all capital assets for inclusion in the budget.

As part of the CRB process, a portfolio analysis is performed. The OCIO submits this analysis with budget recommendations and a list of "at-risk" investments (including major IT investments not receiving passing scores from OMB and other major IT investments identified internally by DOE as requiring additional oversight) to the CRB Board. The CRB Board is comprised of the Deputy Secretary of Energy, the CFO, the CIO, and the senior managers from each of the major organizational elements. Program offices are required to submit proposed budgets including a variety of documents (e.g. Exhibit 300s and 53, budget justification documents, strategic plan/program plans) to the CRB Board. The CRB Board reviews program submissions and analysis from functional areas, including OCIO IT analysis, to make budget decisions.

Investments identified as "at-risk" during the CRB process are subject to budgetary action. The budget decisions resulting from the CRB process are documented in Program Budget Decision (PBD) Memoranda which are provided to program offices. PBD Memoranda provide specific direction to program offices on revisions to proposed

budgets including IT investments. Based on that direction, the program and staff offices revise their respective budgets, business cases, and IT portfolios. At the conclusion of the CRB process, once the program offices have made all required revisions to the IT business cases and portfolios and the OCIO has reviewed the final submission, the draft consolidated DOE IT Portfolio is presented by the CIO to the DOE Management Council for final approval. The final DOE IT Portfolio is submitted to OMB in September of each fiscal year in accordance with OMB Circular A-11 guidance.

1.2.2 Control Phase

1.2.2.1 Control Process Overview

The objective of the Control phase is to ensure that IT initiatives are acquired and managed in a disciplined, well-managed, and consistent manner through timely oversight, quality control, and executive review. The Control phase begins once investments have been selected, budgeted, and received funding. Oversight activities during the Control phase ensure that DME activities are properly managed and that necessary actions are taken when performance and regulatory requirements are not met. DOE Order 413.3 provides the requirements for the acquisition of capital assets, including IT. The requirements include specific, approved program management documentation and specific actions for approvals-to-proceed through the implementation process. Regular reporting requirements and a quarterly Control review process exists at the Department level for major IT investments as defined previously. Investments with total costs below $5 million in prior year PY, CY, and BY are reviewed and managed by their respective program and staff offices.

Major IT investments with total DME costs over $20 million and $5 million DME costs in CY or BY are required to use an ANSI Standard 748-compliant earned value management system (EVMS) and to report EVMS data through PARS on a monthly basis. In addition, these investments are subject to EVMS assessments and quarterly Control reviews by the OCIO. The quarterly Control review scoring criteria includes a specific element for EVM such that any investment required to use an EVMS is scored on the Control review according to their actual EVM performance. Any investments that are out of tolerance must present a corrective action plan to the ITC for review. The ITC will make recommendations to the CIO who will present them, as necessary, to the DOE Management Council for approval and implementation.

Major IT investments with total investment costs between $5 and $20 million in the development phase have the option of using an ANSI-compliant EVMS or a performance management system for management of the investment, but must also report project phase status information through PARS monthly.

Steady State major investments are not subject to EVMS and PARS reporting; however, they must complete all other IT reporting requirements and are subject to OCIO quarterly Control reviews. Each quarter, major IT investments in steady state are required to complete a Control review template reporting actual cost, schedule and performance data. Each investment is required to meet greater than 90% of their cost, schedule and performance goals. Additionally, these investments must certify that they have a qualified project manager, a current security plan, and a completed certification and accreditation, if appropriate.

1.2.2.2 DOE Quarterly Control Reviews

All major investments are subject to OCIO quarterly Control reviews. Non-major IT investments are reviewed and managed within the program offices, but are subject to Department-level review and reporting at the discretion of the CIO. Quarterly Control reviews include review of EVMS data where applicable, and investment cost and schedule status data for investments not subject to EVMS requirements. In addition, all investments must report on project management qualification requirements, as required by the Federal CIO Council guidance. This review assesses the performance of major IT investments ensuring compliance with both external and internal regulations and guidance.

Each quarter, all program and staff offices with IT investments selected for review that quarter, as defined in guidance provided by the OCIO, complete a Control Review report template. After completing the Control Review report template, the program and staff offices submit the forms to the OCIO for review. The OCIO reviews the data and calculates preliminary scores using defined scoring criteria (part of the Department's internal scorecard). Following OCIO's analysis, the ITC reviews the investment's status. The ITC recommends the final score for each investment by evaluating the OCIO analysis, the investment data submitted by the programs and any additional information that may have been provided.

When a program experiences a cost or schedule variance of at least 10%, or fails to meet other defined criteria, the following activities occur:

- OCIO opens a dialog with the program office when reporting appears to indicate an impending breach or issue.
- Upon a breach, the program will be required to submit a corrective action plan/plan of action and milestones (POAM), which the ITC will review and the CIO will approve.
- The ITC assists in the review and monitoring of implementation of corrective action plans/POAMs.

1.2.3 Evaluate Phase

During the Evaluate phase, DOE will determine if implemented IT investments are meeting performance, cost, and schedule objectives; the extent to which the CPIC processes improved the outcome of the IT investments; and whether the operational systems are and will remain in alignment with the DOE EA. Best practices and lessons learned are also captured and reported Department-wide to ensure that other investments may learn from the evaluated investment and to assist with improving the Department's CPIC processes. On an annual basis, the OCIO conducts a self-assessment of its CPIC process to identify opportunities for improvements and to develop an action plan to implement recommendations. The DOE Evaluate process consists of Post Implementation Reviews (PIR) and Operational Analyses.

The purpose of a PIR is to track and measure the impact and outcomes of operational (steady state) IT investments to ensure they meet the program mission and are performing as expected. The ITC approved DOE's initial PIR strategy in February 2005, and approved an updated version in June 2007. Three types of PIRs will be conducted: reviews on newly implemented investments; reviews on mixed life-cycle investments

transitioning into steady state; and reviews on steady state investments. For newly implemented investments, a PIR must be conducted within six to eighteen months of post-implementation. For projects with multiple phases of development, this timeframe will apply to each module that is implemented. Any investment that is transitioning to steady state will be required to conduct a review prior to being permitted to report as a steady state investment. Reporting requirements vary based on the life-cycle stage of an investment.

The final component of DOE's Evaluate phase is operational analysis. DOE policy requires program offices to conduct an operational analysis of steady state investments and investments with operational components at least annually. The results of the operational analysis are reported via Operational Analysis reports and the Exhibit 300 submission, and are validated by the OCIO and IT Council during the yearly Operational Analysis review and annual Exhibit 300 reviews. Operational analysis data is reviewed by the programs to ensure that their steady state components and investments continue to meet all cost, schedule, and performance goals.

The Department's procedures for Select, Control, and Evaluate will be reviewed for completeness, suitability, and effectiveness of the processes and any changes will be incorporated, as necessary.

2.0 LESSONS LEARNED

The OCIO has created and continues to update annually a CPIC process guide, which codifies the lessons learned in developing and implementing an investment management approach to IT acquisitions within the Department. Moreover, the Department's EA program captures "lessons learned" and aligns the Department with the OMB's effort to create a Federal EA.

The DOE Cyber Security Revitalization Plan created a foundation to more comprehensively fulfill the requirements of law in a risk-based, cost-effective, and mission enabling way. The plan described a maturing program based on past lessons learned and recognition that certain specific issues have a higher and more immediate impact on the security posture of the Department. The Program is composed of several components, including:

- **Planning:** Planning is a collaborative effort to understand the threat landscape and identify weaknesses and develop both a long-term strategic plan and an annual tactical plan.
- **Cyber Security Policy and Guidance:** Cyber security policies establish the high-level goals and outcomes for the overall DOE Cyber Security Management Program.
- **Architecture and Technology:** This component includes architectural guidance, enterprise licensing of security tools and products, and a technology review and development process.
- **Services:** These are complex-wide services and include cyber security communications, education and awareness, asset management, advice and assistance, and awards and recognition.

- **Performance Measurement:** Performance measurement activities include compliance reviews and monitoring and cyber security performance metrics.

The implementation of a strong Cyber Security Program will further assist DOE in accomplishing its mission which relies heavily on Information Technology.

3.0 ENTERPRISE ARCHITECTURE PLAN OVERVIEW

3.1 BACKGROUND

The Clinger-Cohen Act of 1996 treats IT as a capital asset, mandating the business-driven analysis of each Federal agency's IT resources to ensure that investments in technology directly support an agency's mission. The establishment and implementation of an effective EA policy and program facilitate the planning, justification, investment in, and management of these technology resources. Clinger-Cohen requires Federal Agency CIOs to develop, maintain, and facilitate "a sound and integrated information technology layer for the executive agency to improve the performance of agency programs and the accomplishment of agency missions through the use of the best practices in information resources management." Subsequently, OMB, in its Circular A-130, issued explicit guidance that requires agency information system initiatives to be consistent with an agency's EA.

While the development and maintenance of an EA is mandated by OMB, DOE approaches EA as a tool for business transformation and progress. Since the passage of these mandates, DOE has steadily built an active EA program to meet the business needs of the Department. The EA program is led by DOE's Chief Architect within the OCIO, but its activities rely heavily on a partnership with the business and IT communities across the Department.

3.2 FRAMEWORK

DOE develops, maintains, and implements a single, cohesive Departmental EA. However, as a large agency with a federated business model, DOE's EA framework naturally mirrors the structure and delivery models of the Department. DOE's EA principles and practices recognize that ownership and control of the EA is a shared responsibility of all of the Department's business units. While some aspects of the architecture are collaboratively defined by the Department as a whole, other architectural elements may be unique at the line of business (LOB) or business unit level.

For clarity in defining policies, roles, and responsibilities, the architecture currently can be envisioned as a three-tier model with Department-level, Program and Staff Office-level, and segment-level EA components. The integration of these three tiers into a functioning whole is an essential element of the Federated EA model. The distinctions among the tiers are as follows:

- **Departmental EA:** Addresses the functions, services and supporting technologies spanning the Department. Development, maintenance, and compliance are the responsibility of all DOE business units; however, the OCIO has a significant oversight role.

- **Program and Staff Office (i.e., Business Unit) Architectures**: Address the functions and supporting technologies unique to individual Program and Staff Offices. The architectures address Program and Staff Office-specific planning issues associated with any requirements established in the Departmental EA. For instance, the Departmental EA may define architectural parameters or requirements for Department-wide business functions or the supporting technologies, but it may require business units to define and detail unique functions associated with their mission.

- **Segment Architectures**: Define the architecture of a group of related Core Mission Business Lines along with their IT investments and their business process improvements. The benefit of this segment type is that it permits identification and implementation of common services among highly related business lines. DOE continues to evolve its segment architectures, applying lessons learned from the segment development process to the development of new segments.

DOE uses the Federal EA (FEA) framework, which comprises architectural layers, specific artifacts, and relationships between the artifacts to provide a model for developing the DOE EA. DOE's EA is consistent with government and industry best practices for EA. The DOE EA builds from the CIO Council's Federal Enterprise Architecture Framework (FEAF) Version 2.1, along with the more recent Version 3.0, and is fully aligned with OMB's FEA reference models. The detailed EA artifact definitions and entity-relationship diagrams are maintained on the OCIO EA portal and are available upon request from the EA Program.

The DOE EA consists of seven key layers.

1. **Business Strategy Layer:** Identifies DOE's strategic goals and objectives. The key benefit of capturing the business strategy layer is to align implementation activities with strategic initiatives and measure organizational performance across the other EA layers.

2. **Business Operations Layer:** Models, from an enterprise-wide perspective, DOE's lines of business, business functions, and sub-functions. It also defines DOE's business organizations, programs and stakeholders.

3. **Applications/Systems and Services Layer:** Defines the set of service domains, types, and components that will provide the information processing capabilities needed to support DOE's business (i.e. the ability to capture, store, access, and manipulate business data and information).

4. **Technology Layer:** Defines the technology standards, services, and products (i.e., the technological infrastructure) that support the secure delivery, exchange, and construction of DOE's business and application services.

5. **Data Layer:** Defines the data and information that support program and business line operations.

6. **Performance Layer:** Ensures the accomplishment of the Department's strategic goals, objectives, and other key measures. The performance layer is related to nearly all of the other EA layers.

7. **Security Layer:** Defines the security elements to be woven into all of the other architectural layers. It encompasses security policies, processes, performance measures, data, and technologies.

Each layer aligns with the applicable OMB FEA reference model as appropriate. The Business Operations Layer, for example, aligns with the FEA Business Reference Model to ensure consistency in design and adherence to a common vocabulary used in defining agency business models. The Data, Applications, and Technology layers employ the Data, Service Component, and Technical Reference Models (respectively). The Business Strategy and Performance layers map to the Performance Reference Model to establish metrics for measuring mission performance and provide "line-of-sight" linkage to the Department's investments and systems.

3.3 DOE EA Repository

In compliance with OMB's position that each agency is viewed as a single enterprise, the DOE has defined its integrated agency-wide enterprise architecture in the DOE Enterprise Architecture Repository (DEAR). DOE configured and deployed the DEAR to facilitate the capture, use, and management of its EA information. DOE maintains all current EA data within DEAR.

The Department uses Telelogic's System Architect as the primary component of DEAR, and relies on the software to capture, maintain, and publish its architecture data and artifacts. In addition, DOE's mission lines of business each have the option of maintaining separate work spaces to support or expand beyond the centrally organized EA efforts. This approach supports a single integrated architecture for DOE and its diverse missions.

3.4 Status of EA

DOE's EA program continues to evolve its EA program by working collaboratively with the DOE Program Offices, laboratories and other business owners to align business and IT functions. OMB's most recent assessment results (Q2 FY 2008) for DOE's EA program illustrate the maturation of the DOE EA with a score of 4.5 out of 5 for completion, use and results of the DOE EA. Moving forward, DOE is focused on continuing the maturation of the EA program through collaboration with DOE business owners to evolve existing segment architectures and develop new segments.

The Department continues to work towards the Target Architecture utilizing the EA Transition Plan. Each line of business identified and implemented opportunities to leverage common business and IT solutions across the Department.

The Agency has taken steps to implement and refine its EA governance organizations and processes. Under the direction of the Chief Architect, the Architecture Review Board (ARB) is working to ensure senior management participation in and control of the EA. The Enterprise Architecture Working Group (EAWG) functions as the principal body for the EA Program. The EAWG serves as the forum for developing the methodology for the architecture development and collection of the architecture artifacts and data. It consists of technical representatives from the program and staff offices and functions as the advisory body on technical architecture issues and repository updates/expansion.

The quarterly review of project performance will focus on earned value and the achievement of the line-of-sight goals the investment supports. The OCIO will review the quarterly information provided and calculate preliminary scores using defined scoring criteria (part of the Department's EA internal scorecard). The Department will continue to assess legacy and developmental systems for alignment with key business, technical, and operational goals and criteria in the DOE Modernization Blueprint. Finally, DOE will focus on maturing the enterprise architecture program and processes, with a goal of reaching level five of the OMB and GAO maturity models.

4.0 CYBER SECURITY ACTIVITY OVERVIEW

Cyber security, like safety, quality, and fiscal prudence is a cornerstone of good operations. Though the Department continues to make significant strides in this area, the increasing number and sophistication of the attacks on the Department's information systems, requires continuous improvement in the cyber security program and its implementation. Recognizing the need and the urgency to ensure the consistent continuous improvement of the Department's Cyber Security Management Program (the Program), the Secretary, Deputy Secretary, Under Secretaries, CIO, and all members of the Department's Senior Management are engaged in integrating cyber security into its missions, thereby ensuring that risks are effectively managed and monitored.

Over the next fiscal year, implementation efforts will improve and upgrade the Department's capabilities. The Program will be updated and improved to meet the anticipated and unforeseen challenges based on the strength of the Department's people, processes, and technologies. The Program will address weaknesses in the Department's cyber security posture, as well as mitigate more immediate issues identified by independent assessments/audits such as those conducted by the Inspector General and the Office of Independent Oversight.

The DOE Cyber Security Revitalization Plan created a foundation to more comprehensively fulfill the requirements of law in a risk-based, cost-effective, and mission enabling way. The plan described a maturing program based on past lessons learned and recognition that certain specific issues have a higher and more immediate impact on the security posture of the Department. The five areas are as follows:

The Program is composed of several components, including planning, policy, management and technology, services, and performance management, as described below. These components are annually reviewed and updated as needed to respond to changes in information technologies and the evolution of the cyber threats. However, it is the mutually reinforcing nature of these elements of cyber security, which emphasize the need for a strong governance structure for the cyber security program. This governance structure allows senior management to see across the program and coordinate with each other across the Department, places responsibility and accountability at appropriate levels, and sets measures and rewards performance.

Longer-term efforts include the following:

- **Planning:** Planning is supported by a collaborative effort to understand the threat landscape and identify weaknesses through compliance reviews and performance measurement. This information is fed back into the planning activities to generate both a long-term strategic plan and an annual tactical plan. Processes and

artifacts produced include a cyber security working group, strategic and tactical plans, and Departmental threat and risk assessment.

- **Cyber Security Policy and Guidance:** The policy component is very closely aligned with both the governance program and the planning component. Cyber security policies establish the high-level goals and outcomes for the overall DOE Cyber Security Management Program. Policy must have enough flexibility to both address security requirements and employ a solution that does not hinder the organization's mission. In the role of a trusted advisor, the CIO is providing high-level guidance, outreach and oversight to complement policy.

- **Architecture and Technology:** Installing well-defined, high-level Departmental structure, processes and principles puts the Department in position to successfully manage the technology it employs. Artifacts stemming from this component include architectural guidance, enterprise licensing of security tools and products, and a technology review and development process.

- **Services:** Sizeable changes to any organization can be difficult. As Under Secretaries and Program Offices adapt to the new processes and policies, it is the role of the OCIO to facilitate that adjustment through various services and through the performance of several key initiatives that protect the entire Department. The aim of these programs is to develop an intelligent and proactive approach to mitigating the security threat to the Department. Processes stemming from this component include cyber security communications, education and awareness, asset management, advice and assistance, and awards and recognition.

- **Performance Measurement:** Performance measurement provides a clear and consistent way to measure success and demonstrate results for senior management. Process and artifacts stemming from this component include compliance reviews and monitoring and cyber security performance metrics.

The Department is committed to continuous improvements of its Cyber Security Management Program and cyber security across the complex. Now more than ever, DOE relies heavily on its information technology to accomplish its mission. Protecting that technology is vital for the Department's success. The Department remains committed to ensuring that cyber security is planned for and funded as part of all agency IT investments. As part of that effort, the Office of Cyber Security is an active participant on a CIO integrated project team that reviews business case summaries for all major IT investments. The reviews evaluate data provided by program manager's including cyber security and privacy information to determine if investments are in compliance with DOE and external requirements.

5.0 INFORMATION TECHNOLOGY BUDGET DOCUMENTS

The Department is required to submit several documents annually with its budget submission. DOE submits the required exhibits listed below electronically using the eCPIC system and ITWeb:.

- DOE IT portfolio (Exhibit 53)
- IT Capital Asset Plans (Exhibit 300)

In addition, DOE submits this IT Capital Plan, its Guide to Capital Planning and Investment Control, and its Information Resources Management Strategic Plan (FY 2009 – FY 2011) with its budget