

•
•
•
•
•
•
•
•
•
•

Annual Report of the Chief Information Officer

Calendar Year 1999



U. S. Department of Energy

Prepared March 2000



• • • • • • • •

Department of Energy

Chief Information Officer 1999 Annual Report

Executive Summary

The Chief Information Officer 1999 Annual Report is prepared in response to the Clinger-Cohen Act of 1996. The Act requires the Chief Information Officer (CIO) to annually review and report to the Agency head on progress made to improve the effectiveness and efficiency of operations and services to the public through the use of information technology (IT). Information technology is an essential component used to accomplish Department of Energy (DOE) missions. During the past year, efforts have focused on the Department's three critical IT priorities: Year 2000, Cyber Security, and Infrastructure and Telecommunications Improvements to Support Corporate Systems. These initiatives and others described in the report illustrate the significant progress made and strategies used to enhance DOE IT capabilities.

The Department's Year 2000 (Y2K) Council, co-chaired by the Deputy Secretary of Energy and the CIO, directed the development and implementation of an overall compliance plan to address internal Departmental activities, domestic energy efforts, and international energy activities. A Y2K Steering Committee was established to implement the Council's direction and coordinate Y2K compliance efforts Departmentwide. All mission critical systems and nonmission critical systems, embedded chips, telecommunications, data exchanges, and workstations are Y2K-compliant. The Year 2000 Rollover was managed by the energy sector and Department of Energy program teams led by the Department's CIO. Few problems were reported and those were quickly corrected.

The CIO initiative to develop and implement a Departmentwide Cyber Security Program was published in the Department's Cyber Security Action Plan, a multi-year roadmap for success. The foundation document supports four pillars of the Cyber Security Program: policy, planning, and performance management; people; operations; and technical capability development. Policies and guidance were issued to provide a consistent governance framework upon which DOE sites construct site-specific Cyber Security Program Plans (CSPP) and manage cyber security efforts. An aggressive training initiative was started to educate new and part-time network and computer system administrators on fundamental cyber security techniques that address system vulnerabilities and increase awareness of cyber security threats.

The DOE Corporate Business Network (DOENET), an Asynchronous Transfer Mode (ATM) network connecting 38 Departmental sites, was deployed in 1999 and provides high-speed access for corporate business data and applications. It also serves as the Departmental Intranet, provides increased protection for sensitive personnel and proprietary data, and facilitates the deployment of client/server and browser-based applications. DOENET implements a security strategy that is consistent with the Department's Security Architecture policies to ensure the privacy and protection of corporate business data and applications.

The DOE Information Architecture Project (DOE-IAP) completed most of the analysis of the DOE business areas by the end of December 1999 and defined the DOE corporate business model and the DOE data architecture. These accomplishments laid the framework for the analysis of DOE corporate IT systems, data, and infrastructure modernization needs. The architecture culminated in a Corporate Systems Implementation Plan which is the basis for requesting an acceleration of funding for corporate systems. The information architecture web site was redesigned and information was updated and reorganized. A working visual model of the as-is architecture was added to the page.

The IT Standards Program fostered adoption of standards that are flexible and in line with the DOE Information Architecture Project in order to enhance information interoperability and data interchange Departmentwide. A Desktop Software Standardization Plan was developed in response to an IT Council proposal and was circulated through the standards adoption process. Further work on the standardization plan is continuing in calendar year 2000. Standards project profiles were developed for Electronic Mail, Digital Signature, and Electronic Commerce and they were posted to the revised IT Standards web site. A review of 143 standards in the DOE Information Architecture Profile of Adopted Standards was completed to facilitate a Departmentwide Sunset Review and update of all adopted IT standards.

The Strategic Information Management (SIM) process, a General Accounting Office sanctioned methodology, is being used by the Department to link business needs and mission requirements with information technology when considering the modernization or development of corporate information systems. In 1999, a SIM process was conducted to consider the need for modernizing the Department's financial systems. Representatives from financial and technical areas of expertise from across the DOE complex participated in this intensive effort. The Business Management Information System - Financial Management (BMIS-FM) Project was then initiated to develop specific requirements and an acquisition strategy based on the business case developed during the SIM process. Additionally, a SIM process business case on the Enterprise Network Infrastructure (ENI) was finalized in 1999 which provided input to the DOE Corporate Business Network implementation. Late in the year, a new SIM initiative was begun for the Collaborative Management Environment (CME), a research and development funding and proposals tracking system.

The Corporate Management Information Program (CMIP) provides funding for and oversight of efforts to modernize major, outdated DOE corporate systems. A rigorous quarterly program oversight/review process was established by the CIO in 1999 to ensure CMIP projects are selected, planned, managed, and funded to provide the greatest potential for success and customer satisfaction. Three of these quarterly reviews were conducted for the Business Management Information System - Financial Management (BMIS-FM) and the Corporate Human Resource Information System (CHRIS), both of which made significant progress in achieving major milestones and goals during the year, a number of which are detailed in the annual report. The CMIP Review Board – composed of the CIO, Chief Financial Officer, and the Director of the Office of Management and Administration (MA) – met twice to review progress and issues of the

sponsored projects and to adjust funding allocations. In addition, the CMIP program office sponsored a very successful project management training program for project managers, team leaders, and CIO staff.

The Frequency Spectrum Management Program is instrumental in sponsoring and negotiating national approval for new, interoperable radio frequency-based technologies to meet DOE's requirements for law enforcement, public safety, and emergency incident response, in support of the President's Critical Information Infrastructure Plan. In 1999 re-engineering activities related to DOE's spectrum management and radio communications systems planning, certification, and licensing processes were initiated through IT modernization and automation. National Presidential and Congressional public safety and wireless telecommunication interoperability initiatives were implemented involving new treaty agreements between several DOE laboratories and state and local governments. These incorporated new scientific breakthroughs for wireless technologies into the regulatory approval process. The DOE provided inputs to international bilateral treaties for mutual interoperability and protection of DOE radiocommunication assets operating near the Canadian and Mexican border zones. The Program continues to forge ahead in new scientific frontiers such as seeking and receiving certification for a new micro-power impulse radar system developed by Lawrence Livermore National Laboratory.

The DOE Electronic Commerce (EC) Program procurement systems modernization effort began implementation of a simplified and paperless web-based system for purchases of \$100,000 or less. This system, DOE/C-Web, is now operational in four Headquarters Program Offices and two DOE Operations Offices. The EC program provided the technical, analytical, and management guidance for the design, engineering, acquisition, implementation, operation and maintenance of DOE's small procurement system. Additional planning began in 1999 to address other procurement modernization areas including grants and contracts.

World Wide Web activities in 1999 focused on improving organizational management and application of the medium as a vehicle for public outreach and service. Working directly with Departmental programs and appropriate staff offices, assistance and support for redesigning the main DOE web site was completed. DOE responded to several malicious attacks on the DOE web site by computer hackers and coordinated actions to ensure the web site was quickly restored and that proper measures were taken to secure the system from future attacks. We coordinated and assisted in developing and deploying security banners pertaining to the use of computers and initiated an effort to produce a public server security guide. The application of best practices and sound design concepts enabled the evolution of content presentation on web sites to meet DOE's functional business support needs. These activities align with the Department's strategic goal of improving communications with customers and the public and meet the Presidential mandate for agencies to do more business via the web.

The Departmentwide Systems Engineering Process Group (DSEPG) revised the Software Engineering Manual, Version 2, of March 1999 to align with the Software Engineering Institute's Capability Maturity Model (SEI CMM) Level 2. The Group also drafted the Information Systems

Engineering Guidance (ISEG), Volume 1, Project Initiation Processes. Assistance was provided by the DSEPG to support the Software Quality Assurance Subcommittee (SQAS) in developing the Software Configuration Management, Risk Management, and Requirements Management Papers. The Group's guidance explains the management of information systems from a DOE high-level view and provides linkage to DOE's information architecture, strategic planning, capital IT investment planning, and oversight reviews.

The Division of Records Management advanced the Department's commitment to manage recorded information in an efficient and effective manner in support of mission accomplishment and accountability. Significant accomplishments by the Records Management Division include publication of Year 2000 Records Management Guidance, development of Design Criteria Standards for Electronic Records Management Software Applications, Technical Standard Project INFT-0001, and revision of the Records Management Order.

In 1999 significant accomplishments by the Directives team under the CIO include development of the electronic Departmental Directives Review and Comment (REVCOM) system, initiation of sunset reviews, and implementation of the DOE Electronic Forms Home Page and Electronic Secretarial Delegations of Authority Home Page for Departmentwide-accessible Delegations.

The Department of Energy's Chief Information Officer is committed to providing strong leadership and collaborating with senior management across the Department to enhance mission accomplishment through the efficient and cost-effective deployment and use of information technology. The accomplishments described in this 1999 Annual Report have positioned the Department to respond rapidly and effectively in leveraging the elements included in the CIO's IT vision: a consistent, enterprisewide IT infrastructure, modern efficient systems for common business functions, increased use of Internet and web technologies, and a Departmentwide architectural framework and guidelines.

Department of Energy

Chief Information Officer 1999 Annual Report

Information technology (IT) has evolved into an essential component of the methods used to accomplish Department of Energy (DOE) missions. As such, IT is a key tool for attaining strategic goals, enhancing efficiency, and reducing costs. Working with Departmental organizations, the Office of the Chief Information Officer (OCIO) has an important role in ensuring the effective use of information technology to help organizations achieve mission goals. Cross-cutting organizations, such as the Offices of the Chief Financial Officer (CFO), Field Integration Council (FIC), and Policy support the Chief Information Officer (CIO) in implementing corporate IT initiatives while balancing technology, security, and the Department's missions. During the past year, development of policies and guidelines provided efficiency and consistency in security and investment.

Initiatives described in this report highlight the progress made and strategies used by the CIO to continue improving DOE IT management capabilities: Year 2000, Cyber Security, Infrastructure and Telecommunications Improvements to Support Corporate Systems, Information Architecture and Standards, IT Capital Planning and Investment Process, Corporate Management Information Program, Strategic Information Management (SIM) process, and several new corporate systems investment initiatives including the Business Management Information System-Financial Management (BMIS-FM), Corporate Human Resources Information System (CHRIS), Frequency Spectrum Management, E-Commerce, World Wide Web, Software Engineering, Records Management, and Directives Management.

1. Year 2000

DOE focused on the Year 2000 (Y2K) transition and worked aggressively to ensure a successful transition. The Department's 420 mission-critical systems and all nonmission critical systems, embedded chips, telecommunications, data exchanges, and workstations are Y2K-compliant. Progress was guided by the Year 2000 Council, established by the Secretary to direct the development and implementation of an overall Y2K plan that addressed internal Departmental activities, domestic energy efforts, and international energy activities. The CIO co-chaired the Year 2000 Council with the Deputy Secretary of Energy. In addition, a Y2K Steering Committee was established to implement the Council's direction and coordinate Departmentwide Y2K compliance efforts.

During calendar year (CY) 1999, the CIO and staff visited more than 30 Departmental sites to appraise progress toward implementing Office of Management and Budget (OMB) and Departmental guidance, assess compliance status of health- and safety-related systems, identify and share Y2K best practices and lessons learned, and improve Departmentwide dialogue on Y2K issues and solutions.

The Department took a phased approach to Y2K preparation activities. Phase I focused on remediation of the Department's 420 mission-critical systems and development of contingency plans should systems experience Y2K-related events. Phase II focused on implementation of additional risk reduction and mitigation measures to ensure that no Departmental mission is compromised due to Y2K transition, as well as development of site business continuity plans to ensure continuation of the Department's core business processes, if mission- or nonmission-critical systems experience Y2K-related failures. Phase III focused on refining business continuity and developing zero-day plans to ensure clear processes to address potential Y2K-induced problems and identify individual roles and responsibilities for monitoring, evaluating, and responding to Y2K-related events across the Department. Phase III also focused on ensuring all remediated, reviewed, and tested systems remain Y2K-compliant should system changes be required.

Phase I is complete. In addition to remediation of the Department's systems, contingency plans were completed, approved, and certified for all DOE mission-critical systems and health- and safety-related systems with Y2K date-related issues. The Department focused particular attention on systems that protect the health and safety of the public, workers, and environment. The Defense Nuclear Facilities Safety Board requested that the Department identify health- and safety-related systems at defense nuclear facilities that may have Y2K compliance issues and provide a schedule for remediation, testing, and independent validation and verification (IV&V). The CIO expanded the scope to include health- and safety-related systems at non-defense nuclear facilities and high/moderate hazard non-nuclear facilities and mandated that systems be subject to the same formality of reporting and rigor of review and testing as mission-critical systems. All of the more than 545 health- and safety-related systems are either Y2K-compliant or Y2K-ready. Positive validation of functionality of all operational health- and safety-related systems was required within 12 hours of Y2K transition to ensure continued safety of the public, workers, and environment.

Phase II is complete. External IV&V activities are complete. Phase II focused on implementation of additional risk reduction and mitigation measures to ensure that no Departmental mission is compromised due to Y2K transition. Business continuity and zero-day plans were developed to ensure continuation of core business processes in the event that mission- or nonmission-critical systems experience Y2K-related failures. Due to the complexity and diversity of the Department's missions and activities and the recognition that Y2K transition posed a unique risk for each site, the Department required 42 business continuity plans and certification by senior line management.

The Department conducted the first formal Y2K readiness exercise during April 1999 to gather lessons learned and best practices data on contingency planning and to establish a baseline for a Departmentwide Y2K drill. Some sites tested contingency plans for most critical systems, while other sites focused on emergency response capabilities for Y2K-related failures. During September 1999, 42 Departmental sites participated in the first Departmentwide Y2K drill. Sites tested various failure scenarios and planned responses to Y2K-related events, rehearsed zero-day procedures, and tested the Department's procedures for reporting Y2K events to Headquarters. Valuable lessons learned from the drill were shared with the CIO and were incorporated into

updates of contingency plans, business continuity plans, and zero-day plans. Two Departmentwide workshops were held to share Y2K lessons learned and best practices. The first workshop was conducted to discuss lessons learned from the April exercise and assist sites in developing contingency and business continuity plans. The second workshop focused on lessons learned from the September drill, outstanding issues regarding business continuity, and zero-day planning activities.

Worst case scenarios addressing all risks associated with the Department's nuclear facilities and waste storage facilities were performed, and contingency plans were put in place to mitigate risks of a Y2K-related system failure. Extensive on-site analysis of the Y2K century date change revealed no foreseeable negative impacts to mission critical systems. The systems involve health and safety of site personnel and/or the population in general, environment, and maintenance of safeguards and security programs. The risk assessment indicates that site systems supporting critical functions have several backup systems or alternate means of accomplishing required functions. Systems in operating facilities have a normal, abnormal, or alarm response and emergency implementing procedures in place that have been tested through the facility operating and drill programs.

Phase III is complete. Phase III involved refining the business continuity and zero-day plans. The Department continued to fine-tune the plans through final transition drills to reflect final staffing decisions as well as the results of Y2K preparation drills within the Department and with the President's Information Coordination Center. Phase III efforts were also focused on managing changes to the Department's systems to ensure that all systems that had been remediated, reviewed, and tested remain Y2K-compliant should changes be required to the systems.

During the transition period the Office of the Chief Information Officer coordinated coverage within the Headquarter's Emergency Operations Center. From December 30 through January 3, around-the-clock monitoring, analysis and reporting was provided. The Lead Program Secretarial Offices (LPSOs), the Offices of Policy, Public Affairs, Intelligence, and the Energy Information Administration participated. In addition, key staff from the electricity, natural gas and oil industries worked with us in the Emergency Operations Center. Activities included monitoring incoming reports from all Departmental sites, analyzing the data, and preparing and forwarding reports to the White House Information Coordination Center. A status report was provided every two hours throughout this period.

The Secretary of Energy was present through the rollover. Constant communication was maintained with the Russian Ministry of Atomic Energy. Secretary Richardson conducted several video conferences with his Russian counterpart, Minister Adamov. Two members of the Minister's staff also worked in the Headquarters' Emergency Operations Center during the rollover.

Staff members from Senator Robert F. Bennett's office, Chairman of the Special Committee on the Year 2000 Technology Problem, and the General Accounting Office were in attendance at

various times during the rollover. The news media were also present, interviewing the Secretary, Deputy Secretary, CIO, and other key officials.

To date, 36 incidents have been reported (out of a universe of over 200,000 systems). Sixteen involved mission-critical or health and safety systems. Procedures which had been developed within the system contingency plans were implemented, and therefore, the impact of any failures was mitigated. As of January 11, 2000, all systems had been corrected. Plans are underway to monitor systems and report any problems over the leap year date of February 29.

2. Cyber Security

The Presidential Decision Directive (PDD-63) for Critical Infrastructure Protection established Agency CIO responsibilities for cyber security. The DOE Cyber Security Program aims to provide the Department with world-class cyber security capability that protects information under Federal requirements and DOE mission needs.

During 1999, the CIO initiative to develop and implement a Departmentwide Cyber Security Program was published in the Department's Cyber Security Action Plan, a multi-year roadmap for success. The foundation document supports four pillars of the Cyber Security Program: policy, planning, and performance management; people; operations; and technical capability development. In addition, policies and guidance were developed to provide a consistent governance framework upon which DOE sites construct site-specific Cyber Security Program Plans (CSPP) and manage cyber security efforts. DOE policy/guidance developed this year includes: Unclassified Cyber Security Program Plan; Guidance Template to Assist Sites in Development of a CSPP; Policies on Mandating Use of Security Warning Banners; Foreign National Access to DOE Cyber Systems; and Password Generation, Protection, and Use. Policies pending issuance are: Incident Warning and Awareness Reporting, Cyber Boundary Protection, Physical Separation of Systems, and Departmental Use of Public Key Infrastructure (PKI). In addition, Full Integration of Unclassified and Classified Cyber Security Policies will be initiated.

The CIO team initiated a quick-reaction cyber security training program to achieve the Secretary's 1999 goal to provide 1,000 DOE cyber system administrators with additional training in cyber system vulnerabilities and proper implementation of cyber system security features. Mobile training teams also conducted cyber threat awareness training with site managers.

The Computer Incident Advisory Capability (CIAC) at Lawrence Livermore National Laboratory is the Departmental focal point for cyber security incident reporting and the backbone of a proactive cyber security capability. CIAC staff was more than doubled in order to enhance the Department's capability to prevent and mitigate effects of cyber attacks. CIAC rapidly distributes cyber system warning advisories and software patches across the Department by coordinating with the National Infrastructure Protection Center and other computer incident response centers.

During CY 2000, the DOE Cyber Security Program will consolidate and tailor policies to maximize benefits of rapidly evolving information technology within a robust and adaptable security architecture. Program objectives include completing development of a cyber security architecture; initiating implementation of a consistent, Departmentwide, baseline perimeter protection and intrusion detection capability; identifying and implementing PKI-based solutions to DOE requirements; and building on pilot PKI initiatives. Additionally, cyber security training will be refined into a sustainable need-based capability that takes advantage of multi-media formats and remote learning technology. Future efforts include leveraging National Laboratories to adapt commercial-off-the-shelf (COTS) cyber security tools, identifying standard solution sets, and filling developmental needs where commercial or other Government Agency cyber security solutions are not available.

3. Infrastructure and Telecommunications Improvements to Support Corporate Systems

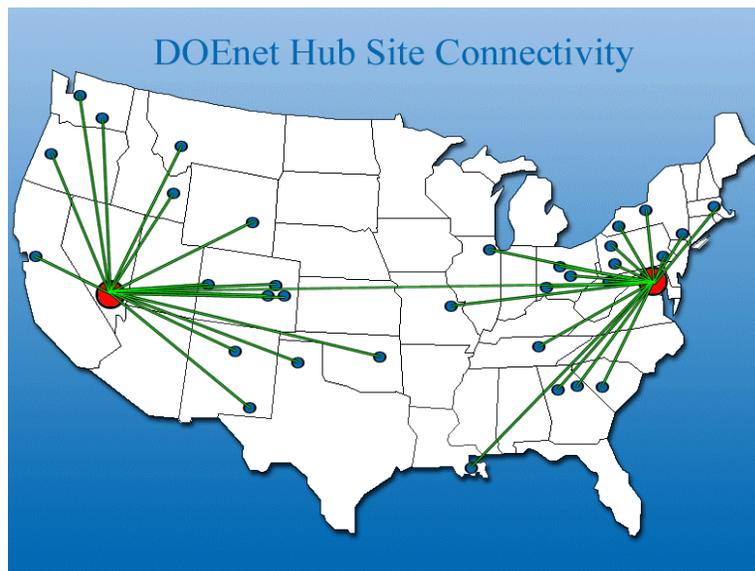
New corporate information systems are driving the need for a corporate telecommunications network that connects DOE facilities with adequate data handling capacity. In 1997, the Department identified a DOE Corporate Network as a top priority to achieve the following objectives: provide high-speed access to corporate data and applications, serve as the Departmental Intranet, increase protection for sensitive personnel and proprietary data, and facilitate the deployment of client/server and browser-based applications.

In 1998, migration began from the existing DOE Business Network (DOEBN), sponsored by the Office of Environmental Management (EM), to a network that supports all Departmental corporate business systems. The DOEBN provided connectivity to 38 sites. The frame-relay network protocol used within the DOEBN supported bandwidth up to 1.544 Mbps; however, many sites identified bandwidth needs in excess of the 1.544 Mbps, and cost savings from consolidating many dedicated circuits could not be achieved without upgrading the network.

Other infrastructure improvements involved the DOE network at Headquarters, which consisted of individual segments attached to a high-speed communications channel backbone. Each segment was developed by and supports a single Program Office. The strategy resulted in numerous, disparate security policies and approaches with attendant vulnerabilities. Accordingly, a centralized firewall implementation strategy was endorsed and activated on September 1, 1998. Sensitive information resources were relocated inside the firewall while resources that require public availability remain accessible outside the firewall.

In 1999, Phase II was initiated, which included specific efforts to develop and implement a security strategy consistent with the Department's Security Architecture policies to ensure the privacy and protection of the DOE Corporate Network (DOENet). Additionally, Phase II included further consolidation of dedicated, long-haul circuits onto the Departmentwide (Corporate) Network. Key accomplishments during 1999 are presented below.

- Completed DOENet Concept of Operations (CONOPS) and Network Security Plan.
- Deployed DOENet asynchronous transfer mode (ATM) hubs in Washington, D.C. and Las Vegas, Nevada.
- Upgraded the existing DOEBN frame relay network by initiating equipment upgrades and installation of ATM circuits at 38 sites.
- Significantly reduced the number of external ISP connections and ensured that any remaining ISP connections are appropriately firewalled, protecting both the site and the network.
- Fully implemented centralized network management.



Corporate Network (DOENet) Infrastructure

All work on the corporate network strengthens the security of the critical component supporting corporate systems. In CY 2000, corporate network convergence upgrades will continue for multiple data networks and long-haul circuits. Upgrades to each site provide corporate network connectivity at a minimum of 1.544 Mbps (T1) ATM service and replace field site data-only telecommunication routers with routers capable of supporting simultaneous voice, video, and data services.

4. Architecture Program

The Information Architecture (IA) Definition Phase concluded with the publication of the Information Architecture Vision, Volume IV, in March 1998. The four volumes of DOE Information Architecture address areas such as the DOE IA framework, conceptual, and process models; a significant baseline analysis; and DOEwide standards, principles, and vision. The Implementation Phase of the Architecture Program began with a pilot IA analysis and planning project in the Office of Science (SC). The pilot was completed in July 1998, and the results were approved by SC management. SC is currently implementing the results of the initial IA-based planning project and will soon begin an effort to extend IA to its field sites.

Based in part on the success of the SC pilot, the DOE Information Architecture Project (DIAP) was initiated in late 1998 and was close to completion in December 1999. DIAP was endorsed by the Information Management Steering Committee (IMSC), the principal advisory board to the Executive Committee for Information Management (ECIM), which is the senior management group for Departmental IT initiatives, and was approved by the ECIM,. The formation of the business representatives team was initiated by direction of the Deputy Secretary. The DIAP architecture process is guiding DOE business representatives from major DOE elements to document core business functions and data requirements; identify opportunities to eliminate redundancies and incompatibilities in data, systems, and technologies; and foster agreement on investment priorities and levels. Four architectures (business, data, applications, and technology) that define the “to be” environment provide the basis for a prioritized migration plan (information technology investments needed to achieve the target architecture).

Integration of the IA resultant migration plan into the Department’s Corporate IT Capital Planning and Investment Process will support new initiatives. The integration also enhances the Corporate Management Information Program (CMIP) by documenting the architectural alignment and priorities of CMIP investments. The Departmental Information Architecture Review Board (DIARB), formed in December 1998, met several times in the year, and consolidation of its functions and responsibilities with the Headquarters (IT) Collaboration Group are being considered. The IA assessment process and the Architectural Assessment module of the Information Technology Investment Portfolio System (I-TIPS) was developed, and testing has begun. Work on the initial module has been completed; however, implementation is on hold pending redefinition and realignment of the assessment process and DIAP outputs.

For January 2000 and beyond, the IA Program focuses on expanding architectural analysis and methods and managing the corporate systems IA implementation. A comprehensive multi-year IA Program Plan was developed and presented to the IMSC in July 1999. The Plan proposes conducting architectural analyses for each LPSO and associated field sites and cross-architectural assessments to develop a detailed, greatly expanded DOE information architecture by FY 2004. The Plan’s approval by the IMSC is pending the DIAP outcome.

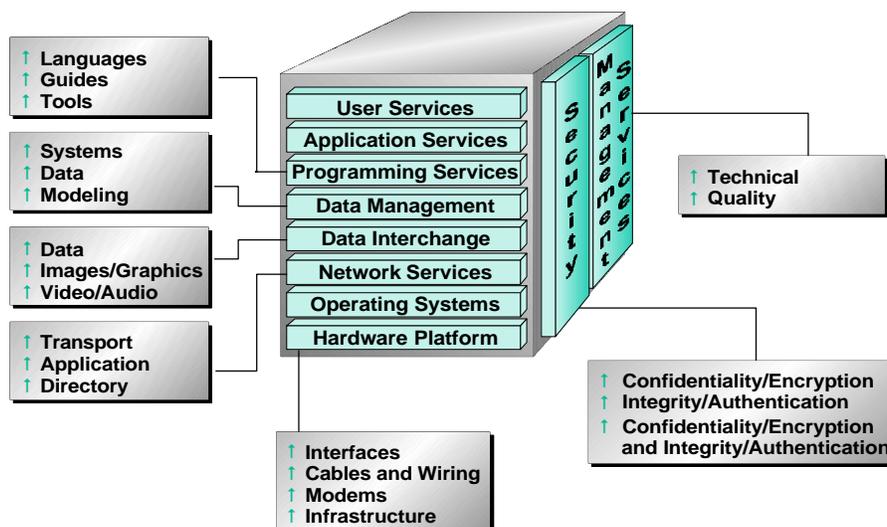
The DOE IA web page has become a benchmark in the Federal government for providing a wealth of information on a successful IA program. Requests for copies of DOE's published IA volumes order from the site average ten sets per week.

5. Architectural Standards

The Departmental IT Standards Program with CIO leadership has evolved to manage, integrate, and centrally coordinate the identification, adoption, and implementation of technology standards in support of the DOE information architecture. The Standards Program applies to all Departmental Elements, including M&O and M&I contractor facilities, laboratories, and Federal field sites. IT standards subject matter experts from across the Department, who often participate in national and international standards bodies, support the adoption process by offering counsel and advice. The goal of the IT Standards Program is to foster adoption of standards that are flexible and in line with Departmental architectural technology directions to enhance technology interoperability and data and information interchange complexwide.

The Program substantiates the Clinger-Cohen Act of 1996 and OMB 97-16, concerning IT architectures requiring a technical reference model and a profile of standards. The DOE Technical Reference Model, developed as a part of the DOE Information Architecture, features ten standards service areas as displayed in the graphic on the following page.

Technical Reference Model



Over 100 standards have been adopted for the service areas and comprise a significant effort of the Program. The published document, DOE Information Architecture Profile of Adopted Standards, September 1997, was the first substantial set of IT standards. At the end of 1999, an internal sunset review of the Profile of Adopted Standards was performed, resulting in the recommendations to update, retire, and add new standards to the profile. The revised profile will be issued in FY 2000.

Also in 1999, an IT Standards Program review was performed to assess its contributions toward the goal of achieving a common information management direction through the adoption of IT standards. Participants responded with an overall rating of 3.9 out of 5 points regarding the usefulness of the Program. Other accomplishments during the year included the adoption of a new DOE Records Management Applications Standard, as well as collaborative work toward the development of a Departmentwide Desktop Standard. The IT Standards web site, which features information about and access to information technology standards, continues to be enhanced, improving usefulness and services to the public and internal DOE customers.

6. Strategic Information Management

The Strategic Information Management (SIM) process, a General Accounting Office sanctioned methodology, is being used by the Department to link business needs and mission requirements with information technology when considering the modernization or development of corporate information systems. The SIM process uses an 8-step approach to produce a business case.

- Establish the scope and boundaries for the project to ensure appropriate focus for the project.
- Build the base case, which identifies the current environment and cost of doing business.
- Examine best practices and industry trends to ensure direction taken is in agreement with best practice principles.
- Identify the high-level requirements of the business function being studied and the needs not currently being met.
- Develop alternative approaches for meeting those needs.
- Perform an analysis of benefits and costs on viable alternatives to show the full costs to implement and the return on investment projected over the lifecycle of the project.
- Recommend the best solution and provide a preliminary action plan to initiate the recommendation.
- Deliver the business case to the CIO and other stakeholders.

The DOE SIM process relies on the knowledge and expertise of a mix of players from both the DOE Federal and contractor communities who represent all areas of the business function being studied. By examining the issues and perspectives of all potentially impacted parties, costs and impacts of the decisions are fully understood before a project is implemented. This collaborative, structured approach assists DOE decision makers in determining the best strategy for

implementing new or enhanced IT to support corporate (or Departmentwide) business needs. It also ensures strategic alignment among key functional elements, which will help realize significant cost savings and business improvement opportunities.

During 1999, the SIM Program accomplished the following:

- A SIM process was completed to consider the need for modernizing the Department's financial systems. Representatives from financial and technical areas of expertise from across the DOE complex participated in this intensive effort. The Business Management Information System - Financial Management (BMIS-FM) Project was then initiated to develop specific requirements and an acquisition strategy based on the business case developed during the SIM process.
- A SIM process business case on the Enterprise Network Infrastructure (ENI) was finalized in 1999 which provided input to the DOE Corporate Business Network implementation.
- Late in the year, a new SIM initiative was begun for the Collaborative Management Environment (CME). This project will improve processes and employ emerging technologies to support management of research and development (R&D) proposal funding, program execution, and project tracking activities. Also, the Nuclear Materials Stewardship Initiative (NMSI) SIM project was initiated to produce a business case for integrating and upgrading DOE's nuclear materials information management and inventory accountability systems. These SIM studies will be completed in calendar year 2000.

7. IT Capital Planning and Investment Process

DOE established the DOE IT Capital Planning and Investment Process in 1998 in response to the Clinger-Cohen Act of 1996, which directs Federal Agencies to use a comprehensive capital planning process for selecting, managing, and assessing IT investments. The Departmental process provides an analytical framework for linking IT investment decisions to strategic objectives, mission achievement, and business plans. It applies primarily to crosscutting corporate administrative and infrastructure initiatives; Program and Field Offices are responsible for similar processes to link IT investments to mission priorities.

The Department has established a two-path (i.e., corporate and Programmatic) approach for IT investment planning. Under the corporate approach, the IMSC and the CIO, with input from the Information Technology Council (ITC), recommend corporate systems modernization initiative projects to the CMIP Review Board. Board recommendations are sent to the ECIM for final approval. Major Programmatic IT projects undergo rigorous program peer reviews to assess the merits of the IT projects to include scientific and/or technical benefits. Together, corporate IT and major Programmatic projects constitute the Departmental IT portfolio.

During 1999, the CIO initiated CMIP Review Board Program reviews and structured Quarterly Technical Reviews of CMIP projects to assess adequacy of planning and performance metrics and ensure schedules were being met. Where appropriate, the CIO provided corrective action guidance as well as guidance to ensure successful development and ultimate full deployment.

Additional significant accomplishments of the IT Capital Planning and Investment Process during 1999 include the following.

- Enhanced Information Technology Investment Portfolio System to assist in DOE Program IT Capital Planning.
- Supported members on Foreign Travel Management System Task Force.
- Enhanced Corporate IT Management process.
- Conducted reviews of the Nuclear Materials Management and Safeguards System.
- Developed analyses of DOE Program and Staff Office IT Capital Planning and Investment Management processes.
- Published revised DOE Guide to IT Capital Planning and Investment.
- Identified Portfolio of Corporate Systems.

For CY 2000, IT Capital Planning and Investment Process implementation plans include providing project manager training for CMIP project managers and developing and issuing a Departmental Management Policy on IT Capital Planning and Investment.

8. Corporate Management Information Program

The Corporate Management Information Program was initiated by the Department in FY 1998 as an investment initiative to replace outdated major DOE corporate systems. CMIP developmental initiatives ensure that the Department has a secure, contemporary, interoperable, and cost-effective corporate information management system.

In 1999, the CIO initiated a rigorous Program oversight/review process to ensure that CMIP projects are selected, planned, managed, and funded to provide the greatest potential for success and customer satisfaction. Activities associated with the Program oversight/review process are described below.

The CIO conducted two cycles of Quarterly Technical Project Reviews during CY 1999. Reviews include briefings on project progress against baseline schedule, deliverables, metrics,

resource requirements (staffing and funding), and customer satisfaction. Some CMIP projects underwent more than two Quarterly Technical Project Reviews due to CIO interest in the project being substantially completed in CY 1999. Action items were closely tracked and monitored by the CMIP Program Manager.

The CMIP Review Board, composed of the CIO, CFO, and the Director of the Office Management and Administration (MA), met semiannually to review progress and issues on CMIP initiatives. During the past year, the CMIP Review Board focused on changes to overall project baselines and resources, including reallocation of CMIP funding to address more critical items in CY 1999, technical review recommendations, ability to sustain projects in the budget out years, and potential adjustment of corporate funds and staff support.

Existing CMIP governing bodies include the ECIM and the IMSC. During the past year, CMIP governing bodies accomplished several review and oversight activities.

The ECIM, chaired by the Deputy Secretary and composed of senior Program and staff officers, conducts periodic reviews for major CMIP Program decisions. In 1999, ECIM oversight ensured that the Department's information management program and investments were consistent with the Department's strategic vision and implemented on mission-oriented performance measures and sound business practices. The ECIM reviewed DIAP initial outcomes including development of a computer based "as is" model of existing DOE systems containing corporate data and a business case. The Committee endorsed the second phase, which involves formation of a team of business experts from the Programs to develop specific architectures. The DIAP culminates with the production of a comprehensive, costed, multi-year, IA-based DOE corporate migration/modernization plan.

The IMSC, co-chaired by the CIO and CFO, convened six times in 1999 to review CMIP progress and ensure that Program decisions were carried out appropriately. IMSC members reviewed proposals on new projects for CMIP funding and made recommendations for approval to the ECIM.

8.A. Business Management Information System - Financial Management

The mission of the Business Management Information System - Financial Management (BMIS-FM) project is to acquire and implement a comprehensive, integrated, computer-based financial management system and adopt standardized, efficient, and effective financial management processes. Two major improvement efforts were initiated to improve access to corporate information in FY 1998. The Corporate Executive Information System (EIS) was designed to meet information needs of executive and senior management, and the Financial Data Warehouse (FDW) was directed at meeting business information needs of Program and project managers and staffs.

In 1999, four improvement efforts were accomplished. Financial and human resource information content in EIS was increased significantly. The EIS users' group was established to help prioritize future content areas. FDW analyses of long-term data needs and alternative production platforms were completed. Critical hardware and additional reporting software were purchased to begin production rollout.

In 1998, a SIM process for BMIS-FM was conducted on financial management functions (i.e., planning, budgeting, accounting, and fiscal services), and a resulting business case was completed in 1999. A COTS-based solution was recommended to replace existing budget and accounting systems, including the Departmental Integrated Standardized Core Accounting System (DISCAS), Management Analysis Reporting System (MARS), Funds Distribution System (FDS), budget formulation systems, and shadow (duplicate) financial systems in most Program and field organizations. Detailed functional and technical requirements analyses and a review of the Department's "account" structure were also initiated in CY 1999 for the acquisition and implementation of new core financial and budget formulation systems.

In FY 2000, the Department will purchase sufficient COTS core financial system software, begin minimal implementation and integration services, and perform training sufficient to support two pilot implementation sites. Hardware and utility software will also be acquired and installed to support the pilot implementation of the core financial system.

8.B. Corporate Human Resource Information System (CHRIS)

Implementation of the first phase of CHRIS on September 27, 1998, as the official personnel system of record provided the Department the flexibility necessary to meet core and priority human resource (HR) mission functions while capitalizing on the latest information technology using PeopleSoft Federal software, a COTS product. CHRIS replaced the PERS portion of the Payroll/Personnel System (PAY/PERS), which was nearing the end of its intended life cycle. DOE became the first Federal Agency to implement PeopleSoft Federal as the official personnel system of record, shutting down a legacy system as a result. The system has been tested and certified as Y2K-compliant along with PAYS (payroll system) and the CHRIS interface created for processing payroll.

CHRIS provides a standardized platform with instant access to human resource and payroll data through the use of client-server and web-based technologies, enabling HR and payroll communities to respond more effectively and efficiently to needs of DOE managers and employees and provide more timely and accurate information for decision-making purposes. During 1999, additional personnel processing enhancements were implemented that significantly reduce the processing time and workload for HR users and improve data integrity. Monthly, quarterly, and semiannual Office of Personnel Management (OPM) reporting requirements were met. Three human resource functions were reengineered and resulted in implementation of a corporate training administration capability in CHRIS, including the development and delivery of

user training for over 200 new users; the Employee Self Service web capability to enable employees to view the earnings statement and personnel/payroll information and electronically update certain personal information directly from the desktop; and a Departmental web-based position-description library for managers and HR Offices to use as a resource tool in preparing positions to expedite the recruitment and staffing process.

Backup and recovery capabilities for the CHRIS production system were successfully implemented and tested during 1999. With the ultimate objective of providing a fully integrated personnel/payroll system using CHRIS, the initial review, fit/gap analysis, and evaluation of PeopleSoft Payroll and Time and Labor were completed to assess the software's readiness and modifications needed for Departmental implementation. A written document was prepared defining the system design requirements to use PS Payroll as a replacement for the legacy PAYS system.

Future plans for CHRIS in 2000 will be to expand the capability for employees to update additional personnel and payroll information from the desktop, upgrade CHRIS with the latest PeopleSoft release to expand and enhance overall functionality, continue to enhance personnel processing functions that will reduce user workload and implement new regulatory requirements, enhance the training administration function, develop reports to manage training information, and begin reengineering studies of other human resource business processes with target implementation of at least one of these. Plans also include development of a detailed implementation plan and defining user requirements for time and attendance, labor distribution, and payroll functions in CHRIS.

As additional components of CHRIS continue to be implemented, projected return on investment will be analyzed through review and analysis of legacy and local HR systems, which the Department has been able to eliminate.

9. Frequency Spectrum Management

The Frequency Spectrum Management Program is the DOE principal voice on domestic and international spectrum-dependent telecommunications and related information technology policy issues. The Program's wide variety of activities have successfully advanced and promoted spectrum-related information technology consistent with DOE objectives and the deployment of new spectrum systems that improve telecommunications in support of DOE missions. Program representatives continue to serve as advocates for DOE and have successfully promoted new policies in the best interests of the Department and the nation. Spectrum use continues to be an essential and growing element of the DOE telecommunications infrastructure, and as such, effective management over the year was critical to supporting mission programs.

During the past year, the Program was instrumental in sponsoring and negotiating national approval for new interoperability requirements for law enforcement, public safety, and emergency

incident response, in support of the President's Critical Information Infrastructure plan. In addition, the Program facilitated the first DOE site to enter into a public safety radio communications-sharing agreement between Argonne National Laboratory and Illinois State police. The Program continued to forge ahead in new scientific frontiers by seeking and receiving national certification for a new technology micro-power impulse radar system developed by Lawrence Livermore National Laboratory. The system uses controversial ultra-wideband radio waves to "see" through solid objects and can aid public safety and law enforcement officials with search, rescue, and apprehension missions. The Program was also instrumental in negotiating a partnership with Ericsson, the second largest manufacturer of wireless telecommunication products, to resolve a standing issue for performing Y2K upgrades and validation testing of critical radio communications systems at five DOE sites.

On the international front, the Program partnered in the development of a United States plan for negotiating a unilateral treaty with Mexico for controlled sharing of the spectrum for emergency response along the 75-mile border zone. The Program also worked on developing an Interim Sharing Agreement with the Canadian Coordinating Agency to modify provisions of the previous Intergovernmental Bilateral Agreement and provide new 50/50 shared land mobile usage along the border. In addition, the Program contributed to the development of new plans and regulations for use of land mobile radio in accordance with national spectrum efficiency mandates, with recommendations to the national spectrum licensing authority and the State Department for the provisions to be reflected in the United States and Canadian spectrum treaty.

10. World Wide Web

CIO-led World Wide Web activities focused on improving organizational web management and improved application of the medium as a vehicle for public outreach and service. Working directly with Departmental Programs, several collaborative and consultative efforts were undertaken that ensured the application of best practices and sound design concepts and enabled evolution of content presentation to meet business support needs. The efforts also identified, supported, and provided information, services, and products that are valued both internally and by the public; improved internal support functions, capabilities, and service standards; enhanced web-based information management functions and tools; and improved internal coordination of content and content management between Departmental functions and organizational components. The activities aligned to and directly supported the Department's strategic goal of improving communications with customers and the public and the Presidential mandate for agencies to do more business via the web.

The Office of the CIO improved security for the DOE Home Page architecture by implementing a dual UNIX server environment with the public server located outside the DOE firewall and the master server located within the firewall. A similar configuration was also implemented for CIO NT-based Home Pages.

11. Software Engineering

The Departmentwide Systems Engineering Process Group (DSEPG) is a collaboration forum focused on information systems project management, engineering practices, and quality assurance to achieve improved and successful software design and system deployments. Monthly meetings were held to discuss Departmental guidance to improve software and systems project management throughout development, deployment, and maintenance cycles. DSEPG includes staff across the complex and its members have expertise in software quality, engineering, and project management of business, technical, and scientific information systems. The group has approved a conceptual model (conceptualization diagram) to guide future efforts. DSEPG is producing guidance that explains the management of information systems from a DOE high-level view, including linkage to Departmentwide information architecture, strategic planning, IT capital planning and investment, and oversight reviews. The CIO Architectural systems engineering staff provides leadership and support for the DSEPG. DSEPG is becoming instrumental in achieving the acceptance, advocacy, and adherence to Department policies, guidance, and processes for maturing the software development and deployment capabilities of Federal and contractor staff.

The DOE Software Engineering Methodology (SEM) was expanded during 1999 to be more inclusive of a total systems implementation approach. SEM was updated with checklists and templates and has led to preparation of the Information Systems Engineering Guide (ISEG) by DSEPG.

In addition, a Policy-Guidance-Metrics-Assessment tool was developed and approved for use within the CIO Office. The tool is a worksheet to aid in the development of policy, guidance, and metrics for measuring the efficiency and effectiveness of the policy. It also supports development assessment criteria for gathering information on the policy's usage, strengths, and weaknesses. Although the tool was developed for use in information architectural engineering practices, it is useful for other functional areas of information technology management. Continuous coordination was established with the DOE International Council on Systems Engineering (DOE INCOSE).

12. Electronic Commerce

The DOE Electronic Commerce (EC) Program is the mechanism to lead, manage, integrate and coordinate Departmental EC efforts. During 1999, the Program provided the technical, analytical, and management guidance for the design, engineering, acquisition, implementation, operation and maintenance of the Departmental small procurement system. The Program also identified actions required to establish EC capabilities consistent with governmentwide policies, DOE information architecture, customer requirements, and applicable laws, rules, and regulations. Through its activities during the year, the Program supported Departmentwide policy development and ensured the coordination of actions with the appropriate Departmental elements.

13. Records Management

Heads of Federal Agencies are required by statute to create records that provide adequate and proper documentation of Agency programs, policies and procedures; effectively manage the records; and carry out appropriate disposition. Objectives of a good records management program are achieved when the Department has access to the information needed to carry out mandated responsibilities in an efficient and effective manner; the ability to produce documentation required by special circumstances, such as audits or court orders without incurring significant expenses; and can preserve necessary records during transition periods of Departmental officials, thus ensuring administrative continuity.

The Division of Records Management has advanced the Department's commitment to manage recorded information in an efficient and effective manner in support of mission accomplishment and accountability. Significant accomplishments by the Records Management Division during CY 1999 are highlighted below.

- Developed and published Year 2000 Records Management Guidance.
- Developed Design Criteria Standard for Electronic Records Management Software Applications, Technical Standard Project INFT-0001.
- Revised and updated the Records Management Order by clarifying roles and responsibilities in order to maintain a cost-effective Departmentwide Records Management Program that complies with the National Archives and Records Administration Act of 1984, as amended.
- Assisted the Office of Defense Programs in the implementation of the Weapons Schedule by conducting training across the Department and reviewing site implementation plans.

During the past year, the Division drafted an electronic records management policy that was reviewed from records management and information technology perspectives. A Departmentwide survey was conducted on current and planned electronic records management software systems use. Survey results and information from DOE Vendor Day on Electronic Records Management Applications assist in establishing criteria for Departmental product endorsement. Endorsed products promote cost-effectiveness by eliminating the need to develop redundant applications and increase information-sharing across sites. The Division is also collaborating with the Office of Counterintelligence to develop electronic mail archiving policies.

14. Directives Management

DOE Directives include policies, orders, notices, manuals, and guides intended to direct, guide, inform, and instruct employees in job performance and enable effectiveness within the Department as well as with Agencies, contractors, and the public. The Directives Management Program includes implementation of the Department's Directives System; management analysis and consultant assistance to DOE organizations on Directives; and development, implementation, operation, maintenance, and enhancement of the automated, online system for DOE Directives.

Significant accomplishments by the Directives team under the CIO during CY 1999 are listed below.

- Developed electronic Departmental Directives Review and Comment (REVCOM) system.
- Initiated Department's Directives sunset review activity phase initiating policy, order, and manual review every two years to determine appropriate action.
- Implemented DOE electronic Forms Home Page for Departmentwide and public forms availability.
- Implemented DOE electronic Secretarial Delegations of Authority Home Page for Departmentwide-accessible Delegations.
- Effectively incorporated the President's Plain Language requirements into directives.

In FY 2000, the Directives Management Program will be under the Office of Management and Administration (MA). Major 2000 initiatives are to fully implement the REVCOM System, eliminating the current hybrid e-mail/memo/fax process and incorporate a revised Field Management Council coordination process into the Directives System.