NAVAL REACTORS DOE DIRECTIVE IMPLEMENTATION BULLETIN 200.1A-127, REVISION 0

Consistent with the Naval Nuclear Propulsion Program (NNPP) overall concept of operations, the following provides specific implementation guidance for DOE Order 200.1A, INFORMATION TECHNOLOGY MANAGEMENT, for those activities under the Director's cognizance. DOE Order 200.1 (series) is implemented subject to the following modifications:

a. The duties and responsibilities delineated in paragraph 5 of the Order are to be carried out by Naval Reactors Headquarters.

b. Information technology capital equipment planning and control and overall IT financial planning and control will be managed in accordance with the latest version of Naval Reactors Implementation Bulletin 413.3-109 and Naval Reactors Procurement Memorandum #43.

c. Oversight of Naval Reactors Prime Contractor implementation of the Order will be provided by the Naval Reactors Laboratory Field Office with additional oversight and direction from Naval Reactors Headquarters.

d. Requests for waivers and exceptions to specific requirements of DOE Order 200.1A or this IB will be submitted to Naval Reactors Headquarters for review and approval.

U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 200.1A

Approved: 12-23-08

SUBJECT: INFORMATION TECHNOLOGY MANAGEMENT

1. OBJECTIVES. The Department of Energy's (DOE) overarching mission, to advance the national, economic, and energy security of the United States and to promote scientific and technological innovation, is enabled, advanced, and reliant on information and information systems that must be effectively managed to ensure mission success.

   This Order supports, and is consistent with, DOE P 413.1, *Program and Project Management Policy for the Planning, Programming, Budgeting, and Acquisition of Capital Assets*, supports the statutory and regulatory requirements provided in the Clinger-Cohen Act, the E-Government Act, the Government Performance Results Act, the Government Paperwork Elimination Act, and Departmental Directives that address effective information technology management of Federal information and information systems, and delineates Departmental requirements and responsibilities to address the following information technology (IT) management areas:

   a. Acquisition, Use, and Management of IT.

      (1) Information Technology Strategic Planning. Conduct strategic planning activities, consistent with performance-based and results-based management and in accordance with the Clinger-Cohen Act Sections 5113 and 5123.

      (2) Capital Planning and Investment Control. Develop, implement, and maintain a Capital Planning and Investment Control process in compliance with DOE P 413.1, Office of Management and Budget (OMB) Circular A-11 Sections 53 and 300, OMB Circular A-130, *Management of Federal Information Resources,* Parts 8 and 9, and Clinger-Cohen Act Sections 5112 and 5122.

      (3) Enterprise Architecture. Maintain an Enterprise Architecture for the life-cycle management of information, information resources, and related IT investments in compliance with OMB Circular A-11 Sections 53 and 300 and OMB Circular A-130 Parts 8 and 9; specifically to:

         (a) Maximize DOE investment in information technology;

         (b) Ensure that information technology is aligned with DOE strategic goals;

      (4) Hardware and Software Acquisition. Ensure that DOE's acquisition, use, and management of IT hardware and software meet program and mission goals as well as promote sound resource management and a more cost-effective government, in accordance with Federal Acquisition

Regulation Part 39, Acquisition of Information Technology, and DOE O 413.3A, Program and Project Management for the Acquisition of Capital Assets; specifically to:

(a) Promote consolidation of software package acquisition, volume purchasing arrangements, enterprise wide agreements and best practices in software implementation, consistent with the SmartBuy program, identified in OMB Memo (M-03-14), *Reducing Cost and Improving Quality in Federal Purchases of Commercial Software*;

(b) Ensure that all Departmental software engineering utilizes a risk and lifecycle based Software Quality Assurance (SQA) program, in compliance with DOE N 203.1, *Software Quality Assurance* and DOE O 414.1C, *Quality Assurance*; and

(c) In accordance with Federal Acquisition Regulation:

1 Establish centralized authorities to coordinate hardware and software purchases,

2 Deploy acquisition strategies for IT hardware and software, designed to take advantage of volume discount savings,

3 Promote use of common hardware and software configurations, where appropriate, and

4 Adopt standard replacement policies to make the best use of existing resources.

(5) IT Operations and Use.

(a) Access for People with Disabilities. Ensure that all Departmental technology is accessible to employees and members of the public with disabilities, in compliance with Section 508 of the Rehabilitation Act.

(b) Web Policy. Ensure that DOE websites comply with OMB Memorandum M-05-04, *Policies for Federal Agency Public Websites*, OMB Circular A-130, and established Departmental Web procedures.

(c) Personal Use. Promote requirements and assign responsibilities for employees' limited personal use of Government resources, consistent with DOE O 203.1, *Limited Personal Use of Government Office Equipment Including Information Technology*.

(d) Public Access. Promote public access to DOE information through the effective use of IT.

(e) Software Piracy. Adopt procedures to prevent illegal or inappropriate use of software licenses.

b. Cyber Security Management. Comply with established security requirements for the protection and control of information, information systems, and matter required to be classified or controlled by statutes, regulations, and DOE Directives, including DOE O 205.1A, *Cyber Security Management*, and DOE P 470.1, *Integrated Safeguards and Security Management*, consistent with the Federal Information Security Management Act of 2002 (FISMA).

c. Spectrum Management. Ensure that all use of radio frequency spectrum is in compliance with Title 47 Code of Federal Regulations (CFR), Part 300, Manual of Regulations and Procedures for Federal Radio Frequency Management and other key publications that provide requirements, standards, and procedures.

d. Records Management. Ensure that a records management program is maintained, consistent with DOE O 243.1, *Records Management Program.*

2. CANCELLATION. DOE O 200.1, *Information Management Program*, dated 9-30-96, expired. Cancellation of an Order does not, by itself, modify or otherwise affect any contractual obligation to comply with the Order. A contractor requirement document (CRD) that has been incorporated into or attached to a contract remains in effect until the contract is modified either to eliminate requirements that are no longer applicable or to substitute a new set of requirements.

3. APPLICABILITY.

a. DOE Elements. Except for the exclusions in paragraph 3c, this Order applies to all Departmental elements, including those created after the Order is issued. (Please refer to www.directives.doe.gov/pdfs/reftools/org-list.pdf for the most current listing of Departmental elements.)

The Administrator of the National Nuclear Security Administration (NNSA) will assure that NNSA employees and contractors comply with their respective responsibilities under this Order. Nothing in this Order will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

The Administrator of the Energy Information Administration (EIA) will assure that EIA employees and contractors comply with their respective obligations under this Order. Nothing in this Order will be construed to interfere with the EIA Administrator's authority to establish EIA-specific policies consistent with Section 205(d) of the DOE Organization Act, Public Law 95-91, or the

Administrator's obligation to ensure limitations on uses and disclosure of data as required by Title V (Confidential Information Protection and Statistical Efficiency Act) of the E-Government Act of 2002, Public Law 107-347, unless disapproved by the Secretary.

The Director of the Office of Intelligence and Counterintelligence (IN) will assure that IN employees and contractors comply with their respective responsibilities under this Order. Nothing in this Order will be construed to interfere with Senior Intelligence Officer's authority to establish IN-specific policies consistent with Director of National Intelligence Directives and Orders and Executive Order (E.O.) 12333, unless disapproved by the Secretary.

b. DOE Contractors .Except for the exclusions in paragraph 3c, the CRD (Attachment 1) sets forth requirements of this Order and must be included in all contracts for the management and/or operation of DOE owned or leased facilities, hereafter referred to as site/facility management contracts, and in all management, operation, and other contracts that require the acquisition, development, modification, or maintenance of computer software and/or IT hardware.

c. Exclusions.

(1) The Naval Nuclear Propulsion Program is excluded from this Order; however, consistent with the responsibilities identified in Executive Order (E.O.) 12344, section 7, the Director of the Naval Nuclear Propulsion Program will ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Order for activities under the Deputy Administrator's cognizance.

(2) Bonneville Power Administration (BPA) is excluded from activities pursuant to objective herein referenced in paragraph 1a(2) and requirement herein referenced in paragraph 4a(2) related to capital planning and investment control. In addition, BPA is excluded from any and all activities pursuant to objective herein referenced in paragraph 1a(4) and any and all hardware and software acquisition requirements herein referenced in paragraph 4a(4) related to Federal Acquisition Regulations (FAR), in accordance with Secretarial Delegation Order 00-033.00A, dated 9-27-02.

4. REQUIREMENTS. Information Technology will be managed consistent with all statutory, regulatory, OMB and Departmental requirements, including the E-Government Act and FISMA, the Government Performance Results Act, the Government Paperwork Elimination Act, and the strategic and operational plans of the Department. Integrated IT management will be administered by the Office of the Chief Information Officer (OCIO) and supported by various working groups fulfilling the following requirements.

a. Acquisition, Use, and Management of IT.

(1) Information Technology Strategic Planning.

(a) Maintain the Information Resources Management (IRM) strategic plan that links IT planning and investment decisions to program mission and goals and establishes Department-wide IT performance goals, objectives, and measures.

(b) Conduct IT performance management, including the development of performance measures that are quantitative and outcome-oriented.

(2) Capital Planning and Investment Control (CPIC).

(a) Implement CPIC processes that effectively manage the selection, control, and evaluation of Departmental IT investments, ensuring prioritization and sound management, including fulfilling OMB reporting requirements for IT investments, as detailed in OMB Circular A-11 for Exhibits 300 and 53.

(b) Ensure that projects and programs are utilizing a systems development lifecycle methodology that effectively manages the development and maintenance of IT systems.

(3) Enterprise Architecture (EA). Oversee a Department-wide enterprise architecture (EA), which supports mission needs and provides business value through collaboration among Departmental elements, including:

(a) Compliance with OMB direction and DOE Directives;

(b) A governance process that promotes integrated business analysis in support of management decision-making;

(c) Alignment with the Capital Planning and Investment Control process; and

(d) Maintenance of a target enterprise architecture aligned with Departmental and Program Secretarial Office (PSO) strategic plans.

(4) Hardware and Software Acquisition.

(a) Perform software asset management including the tracking, licensing, and utilization of DOE's software license inventory.

Develop and maintain procedures to prevent illegal or inappropriate use of software licenses.

(b) Ensure that DOE IT hardware acquisition and replacement practices are consistent with Departmental strategic and operational plans and all statutory, regulatory, administrative, and OMB requirements. They will consist of processes which support DOE in making better hardware decisions and enhancing hardware management.

(c) Oversee Software Quality Assurance programs to ensure that all software owned or maintained by DOE is subjected to formal quality assurance, pursuant to DOE N 203.1 and DOE O 414.1C.

(5) IT Operations and Use.

(a) Ensure software acquisition requirements adhere to the 1998 Amendment to Section 508 of the Rehabilitation Act requirements to provide access for people with disabilities.

(b) Ensure that OMB and established DOE web policy and website requirements are met and all public websites are available to persons with limited English proficiency, per Executive Order 13166, *Improving Access to Services for People with Limited English Proficiency*, and corresponding Secretarial memorandum, Access to Programs and Activities by Persons with Limited English Proficiency, dated 4-11-06.

(c) Promote appropriate personal use of government equipment, consistent with Departmental requirements.

(d) Promote procedures to prevent illegal or inappropriate use of software licenses.

b. Cyber Security Management.

Oversee cyber security policies, procedures, and practices to ensure that they are consistent with OMB and established Departmental requirements.

c. Spectrum Management.

Manage spectrum management processes consistent with regulatory guidance, OMB requirements, and the strategic and operational plans of DOE.

d. Records Management.

Manage records management processes consistent with regulatory guidance, OMB requirements, and the strategic and operational plans of DOE.

5. RESPONSIBILITIES.

a. Chief Information Officer.

(1) Acquisition, Use, and Management of IT.

(a) Information Technology Strategic Planning.

1 Develops and maintains the DOE Information Resources Management (IRM) Strategic Plan.

2 Provides advice and assistance to the Secretary, Deputy Secretary, and other senior management on Department-wide IT management.

3 Reviews the results of internal and external compliance assessments and provides Department-wide direction or guidance, as appropriate.

(b) Capital Planning and Investment Control (CPIC). Provides oversight and manages the CPIC process, including establishing the CPIC process, policies, and responsibilities.

1 Ensures that IT is acquired and information resources are managed consistent with statutory, OMB and Departmental requirements and priorities.

2 Ensures the development, management, and use of an optimal IT portfolio that best supports programmatic needs, minimizes potential risk, and provides the greatest return on investment.

3 Ensures the integration and alignment of the CPIC process with EA, cyber security, budget formulation, investment assessment/prioritization, strategic portfolio review, and other management processes.

4 Provides a means for senior management to monitor investments, and respective milestones, toward measuring progress.

(c) Enterprise Architecture (EA). Establishes and oversees an EA program and procedures to support making optimal decisions and develop and maintain a sound and integrated IT investment portfolio aligned with DOE's mission and strategic business goals.

1 Defines and documents EA through a federated framework for developing, aligning, and implementing IT acquisition,

development, and maintenance activities, working collaboratively with DOE Program management;

2 Identifies opportunities for collaboration, acquisition, and reuse of hardware and software solutions; and

3 Provides reports, analyses, and recommendations to facilitate the strategic planning efforts of DOE Program Secretarial Offices.

(d) Hardware and Software Acquisition.

1 Establishes and maintains Department-wide direction and guidance for systems development lifecycle methodology and processes.

2 Provides a framework for incorporating appropriate new technologies into DOE's IT environment, consistent with Departmental strategic and operational plans and all statutory, regulatory, administrative, and OMB requirements.

(e) IT Operations and Use.

1 Leads DOE E-Government efforts, in collaboration with DOE programs, to improve productivity and service to customers.

2 Establishes DOE requirements and procedural guidance for establishing, operating, and maintaining DOE public websites.

3 Supports and operates DOE's primary website, www.energy.gov, in collaboration with the Office of Public Affairs, which has responsibility for its content.

(2) Cyber Security Management.

Leads DOE's cyber security program, working with DOE Programs and supporting senior management.

(3) Spectrum Management.

Establishes Departmental Directives for the Radio Frequency Spectrum Management Program, including appointing a Department Spectrum Policy and Planning Director and overseeing DOE's compliance with P.L. 107-77 (Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act of 2002).

(4) Records Management.

Maintains the records management program for DOE.

b. Chief Financial Officer.

(1) In conjunction with the CIO, ensures that IT investments meet Government Performance and Results Act performance goals and comply with the Clinger-Cohen Act through appropriate planning and budgeting of resources.

(2) Supports the CIO in the effective financial and project management of IT assets.

(3) Assists in the implementation of requirements, processes, and systems for IT budget administration and program justification.

(4) In conjunction with the CIO, interfaces with the Office of Management and Budget and the Congressional Appropriations Committees in matters related to the Departmental IT budget.

(5) In conjunction with the CIO, develops program performance measures and manages Departmental IT through the Department's performance tracking system.

(6) In conjunction with the CIO, for appropriate IT business lines, budgets for and maintains the Department of Energy Working Capital Fund.

(7) Reviews and makes recommendations regarding Mission Need Statements (Critical Decision-0) for proposed acquisition of new IT capital assets.

(8) Collaborates with the CIO to ensure the incorporation of IT initiatives in the Department of Energy Strategic Plan.

(9) In conjunction with the CIO, provides for and assures the financial integrity, formulation, execution, and analysis of the Department's IT budget.

c. DOE Under Secretaries, including the NNSA Administrator.

(1) Acquisition, Use, and Management of IT.

(a) Information Technology Strategic Planning.

1 Ensure that programs under their authority have implemented this Order.

2 Direct respective contracting officers to reassess their project portfolios so as to ensure that the requirements of this order are implemented and ensure that procurement requests for contracts include appropriate references to this Order and CRD requirements, if necessary.

3 Notify program managers of their responsibilities to define how changes in policy, technology, and workforce will impact their organizations, and implement information technology management requirements to achieve their mission segment architecture.

4 Support the OCIO in the development and implementation of Departmental IT Directives strategy, processes, and procedures.

5 Ensure senior-level Program Secretarial Office representation to serve on, support, and fulfill the membership responsibilities of the IT Council, Architecture Review Board, and EA governance activities.

6 Develop and maintain a Strategic Plan, and corresponding EA, that delineates the strategic direction of Program Secretarial Office programs, projects and organizational IT portfolio.

7 Maintain and use the EA to support strategic planning, budget formulation and execution, capital planning, and hardware and software acquisitions.

8 Support Federal, and Departmental, IT and E-Government initiatives.

(b) Capital Planning and Investment Control. Execute program and office specific processes that support the Department-wide capital planning process, specifically,

1 Demonstrate effective control of the cost, scope, and schedule of investments and corresponding projects;

2 Prioritize investments, based upon performance and results.

(c) Enterprise Architecture. Participate in the development of the DOE EA to support mission needs; provide opportunities for active involvement in continued improvement of the DOE EA; and provide IT business value through collaboration among all Departmental elements by:

1 Participating in the governance process, specifically with EA governance bodies, including the Architecture Review Board and Enterprise Architecture Working Group;

2 Collaborating with contractors to establish direction, issues, and information needs of Departmental EA;

3 Coordinating efforts to integrate a Department–wide architecture, including the development of architectures specific to individual Departmental elements;

4 Supporting the identification of opportunities for collaboration, acquisition, and reuse of hardware and software solutions;

5 Providing EA content to the OCIO and Departmental elements using common definitions, to ensure the effective integration and alignment of EA across DOE.

(d) Hardware and Software Acquisition.

1 Implement Departmental Directives, procedures, and practices for systems development lifecycle management.

2 Encourage centralized coordination of hardware and software purchases, at and above the site level, where possible, so as to take advantage of volume purchasing arrangements.

3 Oversee development and implementation of SQA processes and procedures to ensure that SQA management compliance.

(e) IT Operation and Use.

1 Ensure that all information technology is accessible, in accordance with Section 508 of the Rehabilitation Act.

2 Support the OCIO in establishing DOE direction for the development and implementation of public websites.

3 Ensure that websites are consistent with Federal and DOE policy, as stated in OMB Memorandum M-05-04, *Policies for Federal Agency Public Websites*, and OMB Circular A-130.

4 Verify that each site/facility management contractor's DOE-approved property management system provides

guidance and limitations on personal use of Government resources.

(2) Cyber Security Management.

Leads organizational cyber security programs, consistent with DOE O 205.1A.

(3) Spectrum Management.

Manage spectrum management processes consistent with regulatory and statutory guidance and OMB requirements.

(4) Records Management.

Manage and secure information, records, and IT in accordance with National Archives and Records Administration and DOE policy and procedures.

d. Heads of Departmental Elements (other than Under Secretaries and the NNSA Administrator).

(1) Acquisition, Use, and Management of IT.

(a) Information Technology Strategic Planning.

1 Ensure that programs under their authority have implemented this Order.

2 Direct respective contracting officers to reassess their project portfolios so as to ensure that the requirements of this order are implemented and that procurement requests for contracts include appropriate references to this Order and CRD requirements, if necessary.

3 Notify program managers of their responsibilities to define how changes in policy, technology, and workforce will impact their organizations, and implement information technology management requirements to achieve their mission segment architecture.

4 Support the OCIO in the development and implementation of Departmental IT Directives strategy, processes, and procedures.

5 Ensure senior-level representation to serve on, support, and fulfill the membership responsibilities of the IT Council, Architecture Review Board, and EA governance activities.

6 Develop and maintain a Strategic Plan, and corresponding EA, that delineates the strategic direction of programs, projects and organizational IT portfolio.

7 Maintain and use the EA to support strategic planning, budget formulation and execution, capital planning, and hardware and software acquisitions.

8 Support Federal, and Departmental, IT and E-Government initiatives.

(b) Capital Planning and Investment Control. Execute program and office specific processes that support the Department-wide capital planning process, specifically,

1 Demonstrate effective control of the cost, scope, and schedule of investments and corresponding projects;

2 Prioritize investments, based upon performance and results.

(c) Enterprise Architecture. Participate in the development of the DOE EA to support mission needs; provide opportunities for active involvement in continued improvement of the DOE EA; and provide IT business value through collaboration among all Departmental elements by:

1 Participating in the governance process, specifically with EA governance bodies, including the Architecture Review Board and Enterprise Architecture Working Group;

2 Collaborating with contractors to establish direction, issues, and information needs of Departmental EA;

3 Coordinating efforts to integrate a Department–wide architecture, including the development of architectures specific to individual Departmental elements;

4 Supporting the identification of opportunities for collaboration, acquisition, and reuse of hardware and software solutions;

5 Providing EA content to the OCIO and Departmental elements using common definitions, to ensure the effective integration and alignment of EA across DOE.

(d) Hardware and Software Acquisition.

1 Implement Departmental Directives, procedures, and practices for systems development lifecycle management.

2 Encourage centralized coordination of hardware and software purchases, at and above the site level, where possible, so as to take advantage of volume purchasing arrangements.

3 Oversee development and implementation of SQA processes and procedures to ensure SQA management compliance.

(e) IT Operation and Use.

1 Ensure that all information technology is accessible, in accordance with Section 508 of the Rehabilitation Act.

2 Support the OCIO in establishing DOE direction for the development and implementation of public websites.

3 Ensure that websites are consistent with Federal and DOE policy, as stated in OMB Memorandum M-05-04, *Policies for Federal Agency Public Websites*, and OMB Circular A-130.

4 Verify that each site/facility management contractor's DOE-approved property management system provides guidance and limitations on personal use of Government resources.

(2) Cyber Security Management.

Lead organizational cyber security programs, consistent with DOE O 205.1A.

(3) Spectrum Management.

Manage spectrum management processes consistent with regulatory and statutory guidance and OMB requirements.

(4) Records Management.

Manage and secure information, records, and IT in accordance with National Archives and Records Administration and DOE policy and procedures.

e. Contracting Officer.

Once notified, incorporates the requirements of the CRD into affected contracts. The Statement of Work may include these requirements or the Order may be incorporated by reference into the contract.

f. Information Technology Council (ITC). Acquisition, Use, and Management of IT.

(1) Information Technology Strategic Planning.

(a) Supports the integration of strategic planning with performance indicators, organizational structures, business processes, E-Government, human capital, security, information management programs, budget and capital planning and investment control, IT security management, and EA management in support of DOE mission efficiency and effectiveness.

(b) Assists in developing Directives, resolutions, policies, plans, and procedures regarding information management.

(c) Provides a forum for the dissemination of lessons learned and best practices on IT-related matters, issues, and technologies.

(2) Hardware and Software Acquisition.

Promotes collaboration and effective and efficient acquisition and use of information resources to reduce operational costs and improve the management and execution of IT investments in support of DOE missions.

(3) Capital Planning. Maintains oversight of DOE's Capital Planning and Investment Control process by:

(a) Facilitating the development, maintenance, and implementation of processes that maximize the value of IT acquisitions while assessing and managing the potential risks, in accordance with the Clinger-Cohen Act of 1996 and OMB guidance;

(b) Ensuring full compliance with the E-Government Act of 2002.

(4) Enterprise Architecture. Maintains oversight of the DOE EA by:

(a) Facilitating the development, maintenance, and implementation of a sound and integrated Department-wide EA, in accordance with the Clinger-Cohen Act of 1996, the Federal Information Security Management Act, and OMB guidance;

(b) Assisting in the development of strategic goals and objectives to drive, as appropriate, EA development toward Federal agency-wide initiatives that optimize DOE and Government IT operations and cost;

(c) Identifying opportunities for improving the integration of EA and CPIC processes to mature and enhance processes.

g. Architecture Review Board (ARB).

(1) Oversees the EA program and approves the EA.

(2) Provides recommendations to the OCIO regarding strategies, approaches, products, costs, benefits, cost-benefit feasibility, risks of alternative investment options, and architectural alignment of enterprise and application architecture projects.

(3) Develops recommendations on priorities, common solutions, Directives, policies, plans, procedures, and changes to information management architectures.

(4) Maintains oversight of DOE EA by:

(a) Managing the Departmental Transition and Sequencing Plan, which describes the key planning and implementation activities that support transitioning from the current business environment to the target business environment outlined in the Strategic Plan;

(b) Facilitating communication with all Departmental elements regarding the EA and Program and Staff office architectures;

(c) Reviewing and approving architecture-based recommendations and guidance proposed by the DOE Chief Enterprise Architect for submission to the IT Council;

(d) Reviewing and approving Enterprise Architecture Working Group (EAWG) work products;

(e) Developing and maintaining EA elements and work products, including enterprise reporting.

h. Enterprise Architecture Working Group (EAWG).

(1) Functions as the primary governing body for EA initiatives.

(2) Collaborates to integrate respective program and staff office architectures into the DOE EA.

(3) Performs activities related to the development, implementation, maintenance, and management of the EA.

i. DOE Chief Enterprise Architect.

(1) Acts as the functional EA program manager, providing leadership and direction to groups supporting the EA effort (e.g., EAWG, ARB, Federal employees, contractors).

(2) Coordinates the development, management, and maintenance of the DOE EA.

(3) Submits appropriate EA work products to the ARB and IT Council for their review and approval.

(4) Provides subsequent EA guidance in conjunction with the ARB.

j. Spectrum Coordination Group.

(1) Functions as the governing body for communications among DOE programs and DOE's Radio Frequency Spectrum Management Program.

(2) Provides the primary means for addressing radio frequency and spectrum management issues impacting multiple DOE organizational elements.

(3) Ensures that Department-wide approaches to radio frequency and spectrum management activities are developed and implemented in an integrated and consistent manner.

k. Enterprise-Wide Agreement Integrated Project Team. Acquisition, Use, and Management of IT: Hardware and Software Acquisition.

(1) Functions as the primary governing body for enterprise-wide software initiatives.

(2) Supports efforts to maximize IT buying power, streamline the IT total acquisition lifecycle, and reduce total cost of ownership.

(3) Coordinates the development and implementation of Directives, policies and procedures supporting the identification, acquisition, oversight and compliance of enterprise-wide software.

(4) Facilitates PSO enterprise-wide requirements inclusion into enterprise-wide agreements.

(5) Assesses candidate project alignment with the enterprise architecture.

(6) Identifies, communicates, and collects enterprise-wide opportunities and requirements of common IT assets across all program areas.

(7) Supports the Energy-Wide Strategic Sourcing Program, consistent with the SmartBUY program, to ensure improved efficiency and economies of scale in DOE's acquisition process.

l. Chief Health, Safety, and Security Officer.

Acting as DOE's central element responsible for safety aspects relative to public and worker health, and safety and environmental protection, provides advice and assistance to the Chief Information Officer concerning policy requirements and guidance necessary to implement this directive on software used for safety applications per requirements of DOE O 414.1C, *Quality Assurance*.

6. REFERENCES. See Appendix A.

7. DEFINITIONS. See Appendix B.

8. NECESSITY FINDING STATEMENT. In compliance with Sec. 3174 of P.L. 104-201 (50 U.S.C. 2584 note), DOE hereby finds that this Order is necessary for the protection of human health and the environment or safety, fulfillment of current legal requirements, or conduct of critical administrative functions.

9. CONTACT. Questions concerning this Order should be directed to the Office of the Chief Information Officer, Office of the Associate CIO for IT Planning, Architecture, and E-Government, at 202-586-3705.

BY ORDER OF THE SECRETARY OF ENERGY:

JEFFREY F. KUPFER
Acting Deputy Secretary

CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 200.1A, *INFORMATION TECHNOLOGY MANAGEMENT*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors whose contracts involve Information Resources acquired, created, or used under the scope of its contracts funded by or operated for DOE.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

Program Secretarial Offices (PSOs) are responsible for the lifecycle management of all Information Resources acquired, created, or used under the scope of its contracts and must exercise appropriate stewardship of Information Resources consistent with contract performance objectives and in accordance with DOE efforts referenced herein. Therefore, contractors shall manage Information Resources to support efficient and effective performance of their contract and mission objectives, and in accordance with DOE efforts regarding:

Acquisition, Use, and Management of IT.

1. Information Technology Strategic Planning. Maintain a strategic plan that coordinates IT planning and investment decisions and links contractor-specific missions and goals to the Departmental strategic plan, as well as:

    a. Implement an IT investment decision process that utilizes Enterprise Architecture principles;

    b. Implement and manage IT acquisition processes to achieve cost savings through appropriate IT hardware and software standards, negotiated buying arrangements, and refresh policies.

2. Capital Planning and Investment Control. Develop, implement, and maintain a Capital Planning and Investment Control (CPIC) process, as well as:

    a. Execute program and office specific processes that support Department-wide CPIC efforts by monitoring and demonstrating effective control of the cost, schedule, and performance of investments and corresponding projects;

    b. Implement appropriate internal policies regarding the acceptable use of IT assets;

    c. Prioritizing and selecting investments, based upon performance and results, as part of the budget development process.

3. Enterprise Architecture. Maintain an Enterprise Architecture for the life-cycle management of information resources and related IT investments funded by or operated for DOE.

4. Hardware and Software Acquisition. Ensure the acquisition, use, and management of IT hardware and software funded by or operated for DOE meet program and mission goals to promote sound resource management, specifically to:

   a. Promote consolidation of software acquisition, volume purchasing arrangements, enterprise wide agreements and best practices in software implementation, consistent with the Program Evaluation Management Plan and/or the SmartBuy program.

   b. Implement a Software Quality Assurance (SQA) program that applies a graded, risk-based approach.

   c. Ensure compliance with negotiated contract procurement requirements for IT procurements.

      (1) Deploy acquisition strategies for IT hardware designed to take advantage of volume discount savings.

      (2) Promote use of common hardware and software configurations, where appropriate.

      (3) Adopt standard replacement policies to make the best use of existing resources.

5. IT Operations and Use. Implement and manage IT operations and processes to ensure that information published to Federal service-to-citizens public websites are appropriate, timely, and accessible to the public and individuals with disabilities.

REFERENCES

1. DOE G 200.1-1, *Software Engineering Methodology*, dated 5-21-97.

2. DOE O 203.1, *Limited Personal Use of Government Office Equipment Including Information Technology*, dated 1-7-05, which establishes requirements and assigns responsibilities for employees' limited personal use of Government resources (office equipment and other resources including information technology) within DOE, including NNSA.

3. DOE N 203.1, *Software Quality Assurance,* dated 10-2-00.

4. DOE O 205.1A, *Department of Energy Cyber Security Management Program*, dated 12-4-06. The purpose of the program is to protect all DOE cyber information and information systems by implementing the requirements of applicable laws to maintain national security and to ensure that DOE business operations proceed without security events such as interruption or compromise.

5. DOE O 221.1A, *Reporting Fraud, Waste and Abuse to the Office of the Inspector General*, dated 4-19-08.

6. DOE P 226.1A, *Department of Energy Oversight Policy*, dated 5-25-07.

7. DOE O 243.1, *Records Management Program*, dated 2-3-06.

8. DOE O 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, dated 7-28-06, provides direction to project management for the acquisition of capital assets within DOE, with the goal of delivering projects on schedule, within budget, and meeting mission performance, safeguards and security, environmental, safety, and health standards.

9. DOE G 414.1-4, *Safety Software Guide for Use with 10 CFR 830, Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance,* dated 6-17-05.

10. DOE G 414.1-2A, *Quality Assurance Management System Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance,* dated 6-17-05.

11. DOE O 414.1C, *Quality Assurance*, dated 6-17-05.

12. DOE P 450.4, *Safety Management System Policy*, dated 10-15-96.

13. DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, dated 5-08-01.

14. DOE M 470.4-4 Chg 1, *Information Security*, dated 8-26-05.

15. DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 6-30-00.

16. DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 10-23-01.

17. DOE O 471.3, *Identifying and Protecting Official Use Only Information*, dated 4-9-03.

18. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, dated 4-9-03.

19. DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, dated 3-27-03.

20. DOE O 475.2, *Identifying Classified Information*, dated 8-28-07.

21. DOE M 475.1-1B, *Manual for Identifying Classified Information*, dated 8-28-07.

22. Public Law (P.L.) 93-579, The Privacy Act of 1974, 5 U. S. C., Section 552a, available at http://uscode.house.gov/download/pls/05C5.txt.

23. P.L. 95-91, as amended, Section 644 (42 U.S.C. 7101 note).

24. P.L. 99-508, Electronic Communications Privacy Act of 1986, 18 U.S.C. 2511.

25. P.L. 100-235, the Computer Security Act of 1987, establishes a computer standards program in the National Institute of Standards and Technology (NIST) to provide Government-wide security, including training of persons who manage, operate, and use Federal computer systems.

26. P.L. 106-246, Section 508 of the Rehabilitation Act, as amended by the Fiscal Year 2001 Appropriation for Military Construction, requires Federal agencies to make their information technology accessible to people with disabilities.

27. P.L. 106-554, Section 515, establishes the requirement for an Information Quality Program for information disseminated electronically to the public.

28. P.L. 107-347, E-Government Act of 2002, establishes a Federal Chief Information Officer within the Office of Management and Budget, and establishes a broad framework of measures that require using Internet-based functionality to enhance citizen access to Government information and services.

29. P.L. 107-347, the Federal Information Security Management Act of 2002 (as amended), 44 U.S.C., Chapter 35, *Title III Information Security* (as amended) state that a comprehensive framework will be provided for ensuring the effectiveness of controls over information resources that support Federal operations and assets and for effective Government-wide management and oversight of the related information security risks.

30. Title 5, Code of Federal Regulations (CFR), part 734, Political Activity of Federal Employees.

31. Title 5, CFR part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.

32. Title 10, CFR part 1010.103, Reporting Wrongdoing.

33. Title 41, CFR part 102-193, sets forth policies and procedures concerning the creation, collection, use, documentation, dissemination, and disposition of records maintained by Federal agencies and the National Archives and Records Administration.

34. Title 5, United States Code (U.S.C.) 552, the Freedom of Information Act (Public Law 89-487), as amended, establishes the right of citizens to request information from Federal agencies and establishes a framework of procedures to implement this right.

35. 5 U.S.C. 552a, the Privacy Act of 1974, (Public Law 93-549), as amended, establishes requirements for the collection, maintenance, and dissemination of personal information by Federal agencies.

36. 17 U.S.C. 101-810, the Copyright Act of 1976 (Public Law 94-553), dated 10-19-76, as amended, which establishes the rights and protections surrounding intellectual property.

37. 29 U.S.C. 794d, as amended by the Workforce Investment Act of 1998 (P.L. 105-220), dated 8-7-1998, and http://www.section508.gov.

38. 31 U.S.C. 501 note, addresses shortcomings in financial systems, internal controls, and the use of Federal assets and aims at producing more reliable and useful financial information, in part through the designation of an agency chief financial officer.

39. 31 U.S.C. 1101 note establishes the need for Federal agencies to implement performance measurement programs for their activities, including information management, that use measurable objectives to show whether an agency is getting appropriate value for its investments.

40. 41 U.S.C. Chapter 4 which imposes the responsibility for developing, maintaining, and facilitating the implementation of a sound, integrated IT architecture on Agency chief information officers.

41. 44 U.S.C. Chapters 21, 29, 31, and 33, specify the functions and responsibilities for managing Federal records and the procedures that must be followed to obtain approval for their disposition.

42. 44 U.S.C. Chapter 35 sets forth policies and procedures for the coordination of Federal information policy.

43. 44 U.S.C. Chapter 35 establishes a broad mandate for Federal agencies to perform information activities in an efficient, effective, and economical manner, and specifically recognizes the General Services Administration's role in the acquisition and management of computing resources.

44. 44 U.S.C. Section 3504, which directs Federal agencies to provide for the option of the electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper, and for the use and acceptance of electronic signatures when practicable.

45. 47 U.S.C. Sections 151–614, the Communications Act of 1934 (Public Law 73-416), as amended, provides for the regulation of interstate and foreign communication by wire or radio. In particular, Section 305(a) establishes Presidential statutory authority to authorize operations of radio stations belonging to, or operated by, the Federal Government. Section 606 establishes the war emergency telecommunications powers of the President. Sections 901-928 establish the National Telecommunications and Information Administration (NTIA).

46. Executive Order (E.O.) 12046, Relating to the Transfer of Telecommunications Functions, dated 3-27-78 delegates the Presidential responsibilities for management of the electromagnetic spectrum to the Secretary of Commerce and provides for the continuation of the Interdepartment Radio Advisory Committee to assist the Secretary in this authority.

47. E.O. 12344 and 50 U.S.C. 2406 (Public Law 106-65).

48. E.O. 13011, Federal Information Technology, dated 7-16-96, which integrates provisions of the Clinger-Cohen Act of 1996, the Paperwork Reduction Act of 1995, and the Government Performance and Results Act of 1993.

49. E.O. 13103, Computer Software Piracy, dated 9-30-98, which delegates agencies' authority to establish and adopt procedures to ensure the use of legally licensed software.

50. E.O. 13166 and Secretary Bodman memo, Access to Programs and Activities by Persons with Limited English Proficiency, date 4-11- 2006.

51. Office of Management and Budget (OMB) Circular A-11, Preparation, Submission, and Execution of the Budget provides guidance on preparing fiscal year budget submissions and includes instructions on budget execution.

52. OMB Circular A-130, *Transmittal Memorandum #4, Management of Federal Information Resources,* dated 11-28-00, establishes federal policy for the management of federal information resources.

53. OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* dated 9-30-03.

54. OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act,* dated 8-23-04.

55. OMB Memorandum M-05-04, *Policies for Federal Agency Public Websites*, dated 12-17-04, provides, for the Heads of Executive Departments and Agencies, federal policy guidance for the management of information on agencies' public websites.

56. NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

57. NIST SP 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.

58. DOE priorities, inventories, and schedules are located on the DOE home page under Web Policies at http://www.energy.gov/webpolicies.htm; and additional information is available on Webcontent.gov at http://www.usa.gov/webcontent/reqs_bestpractices/laws_regs/priorities_reqs/process.shtml.

59. DOE domain policy is located on the DOE home page at http://cio.energy.gov/services/dns_policy.htm.

60. OCIO Memorandum for All Headquarters Elements, *Policies for Federal Public Websites*, issued 8-4-06, and OCIO Memorandum for All Program Secretarial Officers, *Compliance with the Office of Management and Budget (OMB) Policies for Federal Public Websites*, issued 10-27-05.

61. CIO TMR-22, Protection of Sensitive Unclassified Information Including Personally Identifiable Information, dated October 17, 2007, located at. http://cio.energy.gov/documents/DOE_CIO_TMR-22_-_SUI_101607_Final.pdf.

62. Usability information is located at http://www.usability.gov/ and http://www.usa.gov/webcontent/usability.shtml.

63. Integrated Contractor Purchasing Team (ITCPT), additional information can be found at https://icpt.llnl.gov/index.html.

64. Electronic Product Environmental Assessment Tool (EPEAT) criteria, additional information can be found at http://epeat.net/.

DEFINITIONS

1. Architecture Review Board (ARB). The principal body charged with coordinating, reviewing and evaluating the implementation of the DOE EA.

2. Business Owners. Departmental entities that have an interest in IT management to support business needs.

3. Capital Planning and Investment Control (CPIC). A systematic approach to managing the risk and returns of IT investments for a given mission.

4. Computer Software Piracy. The use and or distribution of copyrighted computer software in violation of the copyright laws or applicable license restrictions. Common forms include end user piracy, counterfeiting, and hard-disk loading. End-user piracy occurs when an individual or organization reproduces and/or uses unlicensed copies of software for its operations by making more copies of the software than it is licensed for. Counterfeiting is the illegal duplication or distribution of software. Hard-disk loading occurs when a computer hardware reseller loads unauthorized copies of software into the machines it sells.

5. Departmental Element. A Departmental element is defined as a first-tier organization at Headquarters and in the Field. First-tier at Headquarters is the Secretary, Deputy Secretary, Under Secretary, and Secretarial Officers (Assistant Secretaries and Staff Office Directors). First-tier in the Field is Managers of the eight Operations Offices, Managers of the three Field Offices, and the Administrators of the Power Marketing Administrations. Headquarters and field elements are described as follows: (1) Headquarters elements are DOE organizations located in the Washington Metropolitan Area; and (2) "field elements" is a general term for all DOE sites (excluding individual duty stations) located outside of the Washington, DC, Metropolitan Area.

6. Enterprise Architecture (EA). A business-driven plan that describes the current state, future vision, and transitional states of an operation. This is presented in terms of: strategy and performance; business; applications and services; technology; data; and security, all at the end of a two-to-five year planning horizon.

7. Enterprise Architecture Working Group (EAWG). The principal body for DOE and Program Secretarial Office Enterprise Architecture integration initiatives.

8. Electronic Government. Electronic systems and networks that provide the public with access to or interaction with Government entities, services, information, and products without preference in a manner that acknowledges constitutional intent for privacy, security, and, if warranted, anonymity.

9. Hardware. Physical computer and other equipment used to process, store, or transmit computer programs or data.

10. Information Resources. Includes personnel, equipment, funds, and information technology.

11. Information Resources Management. The oversight of the acquisition and use of information resources to accomplish agency missions and to improve agency performance.

12. Information System. A combination of information, computer, and telecommunications resources and other information technology and personnel resources that collects, records, processes, stores, communicates, retrieves, and displays information.

13. Information Technology. Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an Executive agency. For purposes of the preceding sentence, equipment is used by an Executive agency whether the equipment is used directly or by a contractor under a contract with the Executive agency that requires the use of such equipment or requires the use to a significant extent of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services, and resources.

14. Information Technology Council. Designated voting members responsible for coordinating information technology management within DOE.

15. Mission Critical System. Any telecommunications or information system that:

    a. is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996;

    b. is protected at all times by procedures established for information;

    c. has been specifically authorized under criteria established by an Executive order or an Act of Congress to be classified in the interest of national defense or foreign policy; or

    d. processes any information of which the loss, misuse, disclosure, or unauthorized access to or modification would have a debilitating impact on DOE's mission.

16. National Security System. As defined by Clinger-Cohen, any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, the command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions, and excludes any system used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

17. Office of the Chief Information Officer (OCIO). Responsible to ensure that IT is acquired and information resources are managed consistent with statutory, regulatory, and Departmental requirements and priorities.

18. Project Planning. The planning of project technical and management activities that are documented in a project plan. The plan typically describes the work to be done, the resources required, the methods to be used, the procedures to be followed, the schedules to be met, and the way the project will be organized. It includes a list of deliverables, actions required, and other key events needed to accomplish the project.

19. Project Tracking and Oversight. The tracking and reviewing of accomplishments and results against documented estimates, commitments, and plans. Includes the adjusting of plans based on actual accomplishments and results.

20. Quality Assurance.

    a. A planned and systematic pattern of all actions necessary to provide adequate confidence that the item or product conforms to established operational, functional, and technical requirements.

    b. A set of activities designed to evaluate the process by which products are developed or manufactured.

21. Quality Control.

    a. The process by which product correctness is determined and action is initiated when nonconformance is detected.

    b. A line function; the work done within a process to ensure that the work product conforms to standards/requirements.

22. Records Management. The planning, controlling, directing, organizing, training, promoting, and other activities related to the creation, maintenance and use, and disposition of records to achieve adequate and proper documentation of Federal policies and transactions and effective and economical management of agency operations.

23. Requirements Management. In system/software system engineering, the process of controlling the identification, allocation, and flowdown of requirements from the system level to the module or part level, including interfaces, verification, modifications, and status monitoring.

24. Risk Management. An approach to problem analysis that is used to identify, analyze, prioritize, and control risks.

25. Software. All software or software customized for DOE use, proposed for use, under development, or being maintained and used, whether that software was developed in-house, licensed from a commercial vendor for customized use, obtained from another organization, or otherwise acquired. The type of software includes, but is not limited to:

a. administrative/business-oriented software,

b. scientific/engineering software,

c. manufacturing-oriented software, and

d. process control (e.g., programmable logic control instructions).

26. Software License. A contract between a copyright holder and the licensee; a legal contract between a software application author or publisher and the user. The license is somewhat similar to a rental agreement, but it relates to rights to use intangible intellectual property rights instead of tangible goods. Under a typical license, the user agrees to pay for the privilege of using the software and promises the software author or publisher to comply with all restrictions stated in the license agreement.

27. Spectrum Coordination Group. Primary facilitator of communications among DOE spectrum stakeholders and the Spectrum Management Program, as well as the primary means of addressing wireless sand spectrum management issues impacting multiple organizational elements of DOE.