DOJ 2880.1C

INFORMATION RESOURCES MANAGEMENT PROGRAM

Approval Date: May 20, 2011

Approved By: Lee J. Lofthus
Assistant Attorney General
for Administration

Initiated By: Justice Management Division
Office of the Chief Information Officer

FOREWORD

1. **PURPOSE.** This Order establishes Department of Justice (Department or DOJ) policy governing the planning, acquisition, security, operation, management, and use of Information Technology (IT) resources.

2. **SCOPE.** This Order applies to all Information Technology Resources for the Department and components, and IT program personnel, including contractors working on behalf of the Department. National Security Systems operated within the Department are also governed by policies specified by the Office of the Director of National Intelligence (ODNI), which shall take precedence in case of conflict with this Order.

3. **CANCELLATION.** Order DOJ 2880.1B is hereby cancelled.

4. **RELATED DEPARTMENTAL POLICIES AND IRM GUIDANCE.** This Order is supplemented by additional Information Resources Management (IRM) guidance documents, memoranda, and program plans that are developed on an as needed basis and issued as supplements to this Order. These supplements are available on the OCIO webpage (DOJNet). Paper copies of these documents are available from the OCIO.

5. **DEFINITIONS.** Definitions of key terms are provided in Appendix 1.

6. **REFERENCES.** References to selected laws, regulations, and guidance documents are listed in Appendix 2.

TABLE OF CONTENTS

CHAPTER 1. INFORMATION TECHNOLOGY EXECUTIVE LEADERSHIP

1. DEPARTMENT OF JUSTICE CHIEF INFORMATION OFFICER

a. The Paperwork Reduction Act of 1995, the Information Technology Management Reform Act of 1996 (also called the Clinger Cohen Act of 1996), OMB Circular A-130, and various OMB directives require the head of each federal agency to designate a Chief Information Officer (CIO) to head an office responsible for ensuring agency compliance with and prompt, efficient, and effective implementation of the information policies and information resources management responsibilities specified in the legislation.

b. To meet the requirements cited above, the Department has designated a Department Chief Information Officer (CIO) and established the Office of the Chief Information Officer (OCIO) to carry out the responsibilities set forth in legislation and regulations. Except where otherwise authorized by law, regulation, or other policy, the CIO has the authority to set Department-wide IT policy, in all areas of IT governance including enterprise architecture and standards, IT capital planning and investment management, IT asset management, IT budgeting and acquisition, IT performance management, risk management, IT workforce management, IT security and operations, and information security.

c. The Department of Justice CIO (Department CIO), who also serves as the Deputy Assistant Attorney General Information Resource Management (DAAG/IRM) and CIO for the Justice Management Division (JMD), shall advise and assist the Attorney General, the Deputy Attorney General, the Assistant Attorney General for Administration, and other senior staff in order to ensure that the Department plans, acquires, manages, and uses information technology and information resources in a manner that enhances mission accomplishment; improves work processes and paperwork reduction; provides sufficient protection for the privacy of personal information; promotes citizen-centered electronic government; and complies with all applicable Federal laws and directives.

d. The Department CIO shall:

(1) Provide IT leadership for the Department.

(2) Issue Department-wide policies, standards, and guidelines to ensure an effective and integrated approach to IT planning, acquisition, management, and reporting.

(3) Coordinate Federal geospatial investments with other agencies and with State, local, and tribal governments per the requirements of OMB M-06-07.

(4) Develop and implement a DOJ IT Strategic Plan that supports DOJ mission-oriented goals and performance measures.

(5) Assess IT human capital needs and requirements and develop and implement strategies and plans for meeting these needs and requirements.

(6) Review and evaluate:

(a) The performance of DOJ IT programs and projects.

(b) IT funding requests, including reprogramming actions.

(c) The implementation of processes and technologies to carry out information resources management policy(s).

(7) Coordinate implementation of Department-wide information technology policy pursuant to the authorities and responsibilities set forth in this order, and, where practical, in consultation with the Department's CIO Council.

e. As the DAAG/IRM, the Department CIO shall:

(1) Deliver cost-effective, secure, and reliable data processing, computing, telecommunications, internet, and other IT services and operations to the Department on behalf of the Justice Management Division (JMD).

(2) Ensure established IT support arrangements between JMD and those Offices and Boards that do not have IT staffs are delivered as specified in applicable performance level or other service level agreements.

2. DEPARTMENT IT EXECUTIVE BOARDS AND COUNCILS

a. The Clinger Cohen Act of 1996 and OMB Circular A-130 require the Department CIO to design, implement and promote the effective and efficient operation of information resources management processes for the Department.

b. To satisfy these requirements, the Department CIO has established the following executive boards and councils to perform key leadership and oversight roles in the management of the Department's IRM program:

(1) Department IT Investment Review Board (DIRB)

(2) Department CIO Council

(3) Electronic Records Management (ERM) Executive Board

c. The DIRB is chaired by the Deputy Attorney General (DAG), and is composed of the Department CIO (vice-chair), the Department Chief Financial Officer (CFO) and other designated senior executives. The DIRB provides executive-level oversight to ensure disciplined selection and management of the Department's IT portfolio. The DIRB places special focus on monitoring the progress of the department's most critical investments to ensure the Department receives the expected value from these major IT programs and projects. The DIRB Charter, maintained by the Office of the CIO, describes the membership, functions, and operations of the DIRB.

d. The Department CIO Council functions as an advisory board to the Department CIO and meets periodically to support the implementation and management of the Department's IRM program. Each component with a named CIO will be represented on the Department CIO Council by its CIO. Components without a named CIO will designate a representative to the CIO Council. The CIO Council reviews and makes recommendations to the Department CIO on IT strategies, policies, procedures and practices; supports the formulation and implementation of

the Department's IT investment management, enterprise architecture, and IT security programs; provides technical expertise to the Department CIO on component and DOJ IT investments and information sharing initiatives; and shares best practices in IT management. The Department CIO has the authority to establish committees and working groups as necessary to address items of concern to the CIO Council. These committees may be permanent or ad hoc and will be chaired by a CIO Council member. Specific information on the membership, functions, and operations of the CIO Council are defined in the CIO Council Charter maintained by the Office of the CIO.

e. The ERM Executive Board is the governing authority on Information Technology strategic direction, priorities, and long range planning for electronic records management at the enterprise level. The ERM Executive Board reviews recommendations and makes decisions on scope, schedule, and human and financial resources as defined in the governance charter. The ERM Executive Board is comprised of the Department CIO; the DAAG for Policy, Management and Planning; the Deputy CIO for Operations Services or a designee; the Deputy CIO, IT Policy and Planning, or a designee, and the Director of Records Management Policy or a designee. Specific information on the membership, functions, and operations are defined in the Electronic Records Management Governance Charter.

3. COMPONENT IT LEADERSHIP

a. To ensure effective and efficient information resources management processes are established and managed within the Department's components, the Head of each Bureau and Division, as listed in 28 C.F.R. § 0.1, shall appoint a Chief Information Officer (CIO) to manage the information resources for the component. For any other component that has information technology specialist employees AND has an IT investment that requires the preparation of an OMB Exhibit 300, the Component Head shall appoint a CIO. Component Heads that appoint a CIO will inform the Department CIO of the person's qualifications for the position, the organizational placement of the position, and of any responsibilities assigned to the person other than information resources management. Component Heads will determine the organizational placement, roles, responsibilities, and internal relationships for the component CIO with the understanding that the component CIO must be empowered to fulfill the requirements of this order.

b. Actions required by this order that have traditionally been performed by JMD on behalf of those Offices and Boards that do not have their own CIOs and IT staffs shall be continued. Components that depend upon such support from JMD are expected to initiate and frame their IT support requests so as to comply with the requirements of this order.

c. Component Heads shall determine the individual(s) responsible for carrying out all responsibilities listed in this policy as requirements for components.

CHAPTER 2. INFORMATION TECHNOLOGY PLANNING AND MANAGEMENT

1. IT STRATEGIC PLANNING

a. The Paperwork Reduction Act of 1995 and OMB Circular A-130 require executive agencies to develop and maintain a strategic information resources management plan that describes how Department information technology and resources will be managed to support and improve the accomplishment of the Department's missions and strategic goals.

b. To satisfy these requirements, the Department CIO has established an IT strategic planning process that produces and maintains the Department's IT Strategic Plan (ITSP). The ITSP charts a forward course for acquiring and managing the Department's IT resources, and shall be reviewed regularly and updated as needed to support the missions and strategic goals of the Department's Strategic Plan. The Department's IT Strategic Plan shall align with and directly support the Department's Strategic Plan, be comprehensive in scope, and capture all Department-wide IT needs, goals and objectives, and strategies for accomplishing the Department's missions and strategic goals. The strategic planning process is described in the DOJ IT Governance Guide.

c. The Department CIO, through this process, shall:

(1) Align Department IT strategic goals closely with Department missions, goals, and strategic objectives.

(2) Translate Department business needs into IT strategic direction.

(3) Lead and coordinate information sharing between key Federal Agencies, between Federal Agencies and State and local law enforcement and judicial agencies, and between the U.S. and foreign governments.

(4) Lead the effort to standardize and consolidate key Department infrastructure to allow intra-agency and cross-agency sharing of data, information and applications, and to leverage the use of existing and the creation of new, enterprise solutions that will improve mission results.

d. Component Heads shall:

(1) Participate in the development of the Department's IT strategic plan.

(2) Use the Department's plan to guide the formulation of component IT acquisition and management decisions.

(3) Ensure that any component IT strategic plan, if prepared, reflects and aligns with the strategies and goals described in the Department's plan.

2. INFORMATION SHARING

a. Executive Order 13388, dated October 25, 2005, and The Intelligence Reform and Terrorism Prevention Act of 2004 require the Department to develop the means for

sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies.

b. To satisfy these requirements, the Department has established a Law Enforcement Information Sharing Program to promote data exchange between DOJ Components and external partners. This program, in collaboration with the Department of Homeland Security and other Justice programs, has developed information exchange standards to provide standard vocabulary, guidance and processes to promote effective and efficient information sharing across organizational boundaries. Approved DOJ information exchange standards are the National Information Exchange Model (NIEM), as well as the Logical Entity Exchange Specification (LEXS), which is a DOJ-specific implementation of the standard NIEM vocabulary. Additional guidance on use of NIEM and LEXS has been released by the DOJ Office of the CIO.

c. The Department CIO, through this program, shall:

(1) Provide guidance to DOJ Components on the use of information sharing standards and reusable information exchanges.

(2) Represent the Department at inter-agency meetings to ensure that Federal information exchange standards adequately address DOJ requirements.

d. Component Heads shall:

(1) Follow Department guidance for implementing DOJ approved information exchange standards when new systems are being developed or existing systems are enhanced. Use of information exchange standards is essential for exchanges between DOJ Components and between DOJ Components and external partners.

(2) Provide relevant information to the Department's IT Investment Planning process to show implementation of exchanges that conform to DOJ approved standards.

(3) Require the use of DOJ approved information exchange standards in request for proposal (RFP) language with commercial vendors and in grant language with state, local and/or tribal governments, as appropriate. RFP language can be found at the JMD Procurement Services Staff webpage.

(4) Include in their respective Systems Development Life Cycle (SDLC) guidance, in either a new or existing control gate, the requirement that IT programs' implementation of appropriate information exchange standards is reviewed and approved by the Component and Department.

3. IT ENTERPRISE ARCHITECTURE

a. The Clinger Cohen Act of 1996 and OMB Circular A-130 require the Department CIO to develop, maintain, and facilitate the implementation of a sound and integrated information technology architecture for the Department, document the Department's enterprise architecture (EA), and report significant changes to OMB.

b. To satisfy these requirements, the Department CIO has established an Enterprise Architecture (EA) Program. The DOJ EA program, its methodology and governance are defined in the EA Program Manager User Guide (EA PMUG).

c. The Department CIO, through this program, shall:

(1) Ensure the Department's EA framework encompasses all of the Department's missions and strategic goals and is aligned with the Federal Enterprise Architecture (FEA).

(2) Ensure that Department IT investments are consistent with Federal, Department, and Component enterprise architectures.

d. Component Heads shall:

(1) Participate in the development of the Department target architectures to ensure component business and mission requirements are satisfactorily supported.

(2) Ensure solution architectures developed to meet component mission and business needs conform to Department EA policy and requirements.

(3) Ensure component investments are consistent with Department and Component enterprise architectures.

4. IT PERFORMANCE MANAGEMENT

a. The Paperwork Reduction Act of 1995, the Clinger Cohen Act of 1996, and OMB Circular A-130 require the Department CIO to establish goals for improving the contribution that information resources management provides to program productivity, efficiency, and effectiveness; to institute performance measures and management processes that monitor actual performance; and to ensure that performance measurements are prescribed for information technology used or acquired for the Department.

b. To satisfy these requirements, the Department CIO has established a performance management process that evaluates implementation of performance measures; reviews the results delivered by the Department's IT investments; and assesses the contributions of IT investments toward improving the Department's mission and business performance.

c. The Department CIO, through this program, shall:

(1) Develop strategic performance goals and measures in consultation with the Components that align with the Goals and Objectives stated in the IT Strategic Plan.

(2) Evaluate performance results of key IT investments to determine progress toward achieving the Department's goals.

d. Component Heads shall:

(1) Ensure that performance measures are established for all investments within their respective IT investment portfolios and that the measures are used to monitor and evaluate investment performance.

(2) Monitor and evaluate performance results of component IT investments and take appropriate action to ensure those IT investments contribute to achieving strategic goals and objectives.

5. IT INVESTMENT MANAGEMENT

a. The Clinger Cohen Act of 1996 and OMB Circular A-130 require the Department CIO to plan, manage, and evaluate the Department's IT investments to ensure taxpayer value and return.

b. To satisfy these requirements, the Department CIO has established the IT Investment Management (ITIM) Program. The program manages the repository of IT investments for the Department and the annual IT investment process for new appropriated funds, and responds to external inquiries regarding the Department's IT investment portfolio. The ITIM Program and the investment management process are described in the DOJ IT Governance Guide.

c. The Department CIO, through this program, shall:

(1) Establish and maintain a department-wide IT investment management process that evaluates and manages department-level IT investment portfolios to ensure taxpayer funds are used wisely to further the Department's strategic plan and mission.

(2) Integrate the Department's IT investment management process with the Department's budget process and manage the IT budget formulation process.

d. Component Heads shall:

(1) Evaluate and manage component-level IT investment portfolios to ensure taxpayer funds are used wisely to further the Component's strategic plan and mission.

(2) Submit accurate annual requests for appropriated funds for IT investments on time to support the Department's budget review and formulation processes.

(3) Provide accurate information regarding their IT investments as requested by the Department CIO to respond to external inquiries.

6. IT PROGRAM AND PROJECT MANAGEMENT

a. The Clinger Cohen Act of 1996, OMB Circular A-130, and additional guidance directives require the Department CIO to monitor the performance of information resource investments, to ensure that major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle and continue to deliver intended benefits to the agency and customers, and to implement effective management processes for IT acquisition programs and projects. The Department CIO and Component Heads are encouraged under OMB Circular A-11 §300 to reduce project risk by developing a segmented approach to large projects as part of their proposed cost goals.

b. To satisfy these requirements, the Department CIO has established a department-level Project Management Program to define Department-wide guidelines for IT investment development planning and program management and to monitor those investments that are most critical to the Department's mission and are most at risk. The program has implemented a project oversight process for monitoring the development and implementation of selected investments and evaluating project progress and risk. The project oversight process is described in the DOJ IT Investment Baseline Management Guide.

c. The Department CIO, through this program, shall:

(1) Develop and implement department-wide project management guidelines, including a standardized DOJ SDLC methodology.

(2) Issue guidance on the implementation of Earned Value Management (EVM) and on IT Investment Baseline Management within the Department.

(3) Require and enforce Earned Value Management (EVM) training for all personnel with investment oversight and program management responsibilities.

(4) Evaluate major IT projects periodically to monitor their progress against their original plans, assess project risks, and ensure appropriate corrective actions are implemented, when necessary.

(5) Ensure that performance measurement baselines are established for major IT investments.

(6) Support and monitor a project management training and development program for project managers by ensuring project managers are qualified and certified, as necessary, to manage IT projects.

(7) Monitor and approve changes to the performance management baselines of major IT investments via the use of performance management systems and issue guidance on the process for managing baseline changes; and ensuring the implementation of Federal IT Dashboard reporting requirements.

(8) Specify requirements for use of industry and government Best Practices for program and project management including use of independent verification and validation and Integrated Program Teams, when appropriate, to ensure effective planning, risk reduction, and assessment of project outcomes.

d. Component Heads shall:

(1) Implement the Department's project management guidelines, including the standardized DOJ SDLC methodology for all major development/ modernization/enhancement (DME) IT projects or obtain approval from the Department CIO to use an alternative methodology.

(2) Implement procedures to improve IT project planning and execution and fully implement ANSI 748-compliant Earned Value Management Systems (EVMS) for major development/modernization/enhancement (DME) IT Projects.

(3) Implement Department guidance for use of EVM including the use of EVMS compliant with ANSI/EIA-748 for all major IT projects.

(4) Ensure that development/modernization/enhancement projects employ a modular development approach that will deliver usable functional components or capabilities in a timely manner, typically in less than 12 months and no more than 18 months after project start.

(5) Establish and validate performance measurement baselines with clear cost, schedule and performance goals through independent assessments or Integrated Baseline Reviews.

(6) Measure project progress and manage projects baseline goals through the use of EVM, or for steady state projects, perform operational analyses.

(7) Implement Department IT Investment Baseline Management guidance on performance measurement baseline maintenance and change processes, including requesting approval from the Department CIO for changes to major IT project baselines, and performing an Integrated Baseline Review whenever a new project baseline is established or a project is rebaselined.

(8) Support DOJ OCIO system surveillance reviews to ensure that EVMS for designated projects continue to meet the ANSI/EIA -748 guidelines.

(9) Submit periodic progress reports for all major DME programs and other designated projects as directed by the Department CIO.

(10) Assign a qualified project manager to each IT project.

(11) Implement appropriate internal project management, reporting, and monitoring processes for all major IT development and operations projects, and apply industry and government best practices, including use of independent verification and validation and Integrated Program Teams, when appropriate or when directed, to ensure effective planning, risk reduction, and assessment of project outcomes.

(12) Avoid investment duplication by leveraging Department, inter-agency and government-wide investments to support common missions or other common requirements.

e. The Department CFO, through this program, shall:

(1) Evaluate all financial system modernization projects (as defined in OMB Circular A-127) including all business system projects in conjunction with financial system modernization projects, to ensure compliance with OMB guidelines as detailed in M-10-26.

7. IT EXECUTIVE OVERSIGHT

a. The Clinger Cohen Act of 1996, OMB Circular A-130, and OMB Circular A-11 require the Department CIO to establish a process that provides the means for agency senior management to obtain timely information regarding the progress of the Department's investments in information systems, and to advise the Attorney General regarding whether to continue, modify, or terminate a program or project.

b. To satisfy these requirements, the Department CIO has established a department-level Executive Oversight Process that is administered by the DIRB. The process is described in the DOJ IT Governance Guide and the DIRB Charter.

c. The Department CIO, through this process, shall:

(1) Ensure the DIRB is engaged to effectively oversee the Department's IT program.

(2) Brief Department senior leadership on the Department's IT investment requirements and plans.

(3) Identify important IT programs to be monitored and evaluated by the DIRB on an ongoing or as required basis.

d. Component Heads shall:

(1) Provide information necessary to brief the DIRB regarding component IT investment requirements.

(2) Support DIRB reviews of selected component IT programs, as required.

(3) Ensure program compliance with DIRB decisions and instructions for corrective actions, when assigned.

8. IT ACQUISITION MANAGEMENT

a. Federal Acquisition Regulations Part 39 (FAR), the Justice Acquisition Regulation, OMB Circular A-130, OMB Circular A-11 , and Department Procurement Guidance memoranda require the department to publish uniform policies and procedures for acquisition of IT systems and services. Acquisitions of Information Technology for National Security Systems must be conducted in accordance with 40 U.S.C.§ 11302. Additionally, the department is committed to sustainable environmental stewardship of it's Electronic Assets. Accordingly, the department will develop the necessary policies, guidance, reporting metrics, and other documents and tools required to meet federal mandates and regulations with regard to stewardship of its Electronic Assets. This includes but is not limited to adherence to Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance"; Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management", and the "Federal Acquisition Regulation" Title 48 Part 23.", which requires executive agencies to implement environmental and energy saving policies and procedures to reduce the environmental impact of electronic equipment throughout all life cycle phases.

b. The Department CIO, through this policy, shall:

(1) Define and publish department-wide policies for IT acquisition, including the use of OMB Exhibits 300 and 53 to document the acquisition of IT investments.

(2) Develop formal, written, documented green purchasing plans, policies and/or procedures for the implementation of the statutory and executive order requirements to purchase so-called "green" products and services.

(3) Per OMB Memorandum M-04-08, certify in writing, in conjunction with the Senior Procurement Executive (SPE), that the department has no information technology acquisitions that duplicate the Administration's e-Government initiatives.

c. Component Heads will ensure compliance with this policy, and shall:

(1) Use acquisition planning to direct procurements throughout the life cycle of major IT projects.

(2) For software purchases, components shall use DOJ Enterprise License Agreements (ELAs), Blanket Purchase Agreements (BPAs) and contract vehicles if economically advantageous. Significant software purchases should be negotiated directly by DOJ and not purchased on DOJ's behalf by an integrator. For hardware and services, components shall use DOJ Blanket Purchase Agreements (BPAs) and contract vehicles if economically advantageous. If a DOJ vehicle is not used, components should use General Services Administration (GSA) ELAs, BPAs and contract vehicles for software, hardware and services if economically advantageous.

(3) Adhere to Office of Management and Budget (OMB) directives for procuring IT products and services. For additional guidance see the Department Procurement Services Staff webpage.

(4) Produce Statements of Work (SOWs) that reference and require compliance with all relevant Federal, Department, and Component IT policies, the Department Enterprise Architecture, and applicable Department standards, where compliance is required for the acquisition of IT products and services.

(5) Ensure that program managers for major acquisition programs assess program risks and implement independent verification and validation (IV&V) reviews to evaluate program plans and results, when appropriate.

(6) Require contractors, through SOWs, to use an earned value management system to monitor and report on project cost, schedule and performance outcomes for major IT development/modernization/enhancement projects.

9. IT ACCESSIBILITY

a. The department must comply with the requirements of the Workforce Investment Act of 1998, 29 U.S.C. § 794d (Section 508 of the Rehabilitation Act of 1973), as amended (Section 508) and OMB Circular A-119, and all relevant statutes, regulations, and guidance, to ensure that Department information technology is accessible by Federal employees, contractors, and members of the public.

b. The Department CIO, through this policy, shall:

(1) Develop and issue Section 508 accessibility policy guidance, as needed.

(2) Appoint a Department Section 508 Coordinator

c. The Department Section 508 Coordinator shall:

(1) Facilitate department compliance with Section 508 of the Workforce Investment Act of 1998. Requirements and implementation guidance for this Act are available at Section508.gov.

(2) Develop and manage a Section 508 complaint process.

(3) Respond on behalf of the department for Section 508 reporting requirements.

d. Component Heads will ensure compliance with this policy, and shall:

(1) Ensure the implementation of Government-wide and Department policies regarding compliance with Section 508 within their respective components when acquiring, developing, and maintaining IT systems and equipment.

(2) Appoint a Component Section 508 Coordinator to serve as a point of contact for Section 508 issues, and inform the Department CIO of that person's name and contact data.

10. IT SECURITY MANAGEMENT

a. The Federal Information Security Management Act of 2002 and OMB Circular A-130, Appendix III, and OMB guidance regarding FISMA reporting requirements, require the Department CIO to develop and manage an agency wide Information Technology Security Program to ensure Department systems are secure.

b. To satisfy these requirements, the Department has established an IT Security Program to ensure compliance with these laws and regulations. The policies, standards, and procedures developed as part of this program apply to all DOJ IT systems. DOJ IT systems that process National Security Information (NSI) must meet any additional requirements specified by the interagency Committee on National Security Systems (CNSS). DOJ IT systems that process Sensitive Compartmented Information (SCI) must meet any additional requirements specified by the Director of National Intelligence (DNI). If there is a conflict in requirements for systems processing NSI and/or SCI, the CNSS or DNI requirements shall govern. Components shall use NIST SP 800-59, "Guideline for Identifying an Information System as a National Security System," to identify National Security Systems.

c. Department and Component roles and responsibilities for implementing IT security requirements are set forth in the Department's Information Technology Security Order DOJ 2640.2.

11. IT INFRASTRUCTURE AND ASSET MANAGEMENT

a. The Paperwork Reduction Act of 1995 (PRA), the Clinger Cohen Act of 1996, the Privacy Act of 1974, Federal Information Security Management Act of 2002 (Title III of E-Gov), and OMB Circular A-130 require the Department CIO to manage information resources to increase program efficiency and effectiveness; implement and enforce applicable information technology management policies, principles, standards, and guidelines; provide for identifying information systems investments

that result in shared benefits or costs and prevent redundancy of existing or shared IT capabilities; and safeguard the Department's IT assets.

b. To satisfy these requirements, the Department CIO has established an Asset and Infrastructure management program to support components throughout the Department of Justice. The program strives to align the Department's infrastructure with the Department's enterprise architecture, leverage common infrastructure for use across the Department, as well as comply with federal guidelines for IT security and asset management. Consideration of and use of the Department's shared Information Technology infrastructure shall be made before any new investments or acquisitions of IT infrastructure are considered.

c. The Department CIO, through this program, shall:

(1) Provide an Information Technology infrastructure to support components throughout the Department. This infrastructure shall be consistent with the Department's enterprise architecture, and with federal guidelines for IT security and management.

(2) Ensure that Department and Component-provided IT infrastructure resources comply with all applicable federal, Departmental, and Component IT policies, guidance and standards, and comply and align with the DOJ Enterprise Architecture.

(3) Approve any deviations from applicable policies, guidance and standards.

(4) Define and publish Department-wide policies and guidance regarding infrastructure and asset management.

d. Component Heads shall:

(1) Ensure that OCIO-provided IT infrastructure resources are used for Component computing services unless a written waiver is received from the Department CIO. A current list of departmentally provided IT infrastructure resources is available on DOJNet at: http://dojnet.doj.gov/jmd/irm/ocioservices.php.

(2) Ensure that component-provided IT infrastructure resources meet the federal contingency planning requirements of either being incorporated in a Departmental (DOJ) Continuity of Operations Plan (COOP) or having an up-to-date and effective component COOP.

(3) Ensure that Components have an effective IT Contingency Plan (ITCP), for their IT infrastructure resources, that is continually exercised (at least one time per year) and maintained in an up-to-date state; store copies of the up-to-date ITCP for each respective system at the primary and alternate site locations.

(4) Comply with all Department policies regarding management of IT infrastructure assets and equipment.

12. IT WORKFORCE MANAGEMENT

a. The Clinger Cohen Act of 1996 requires the Department CIO to assess the requirements established for Department personnel regarding knowledge and skill in

Information Resource Management, and to ensure personnel at the executive and management level meet these requirements to determine their adequacy for facilitating achievements of performance goals. The Department CIO must also rectify any deficiencies in meeting those requirements, and develop strategies and specific plans for hiring, training and professional development. OMB Circular A-130 requires the Agency Head to ensure the Department develops a well-trained corps of information resource professionals.

b. To satisfy these requirements, the Department CIO shall:

(1) Determine the Department's IT human capital requirements.

(2) Assess IT workforce skills and competencies and determine gaps and areas for improvement.

(3) Develop strategies and plans for recruiting or training current staff to satisfy required skills.

(4) Establish qualifications requirements for critical IT management staff positions.

(5) Monitor Component compliance with Department policies and guidelines.

c. Component Heads shall:

(1) Ensure compliance with the requirements of the DOJ Human Capital Strategic Plan.

(2) Ensure IT project and program managers and other IT professionals are qualified or certified according to OMB and Department requirements as specified by Federal and Department directives.

13. PROTECTION OF PRIVACY AND PERSONALLY IDENTIFIABLE INFORMATION (PII)

a. Section 208 of the E-Government Act of 2002 and the Privacy Act of 1974, along with OMB and Department guidance and policies, promote the use of electronic government services to individuals, while also regulating the handling of PII. These authorities require the Department to incorporate privacy and civil liberties assessments into the Department's information technology processes. Specific requirements for privacy reviews and approvals are set forth in Order DOJ 3011.1A "Compliance with the Privacy Requirements of the Privacy Act, the E-Government Act, and the FISMA" and must be followed in order to ensure compliance with the mandates contained in such authorities.

14. INFORMATION COLLECTION MANAGEMENT

a. The PRA, 44 U.S.C. Sections 3501-3520, and Title 5, C.F.R., Part 1320 – Controlling Paperwork Burdens on the Public require the Department CIO to minimize the paperwork burden on private citizens while ensuring support of the Department's mission by establishing a program for reviewing information collections.

b. To satisfy these requirements, the Department CIO has established a PRA Program to ensure that information collection requirements are limited to the minimum necessary for protection of the public, policy development, effective management planning, and external reporting; information collections are conducted using the most efficient, effective, and economical manner possible and promote the use of information technology; information collections in violation of the Act are resolved immediately, as described in the Title 5, C.F.R., Part 1320; and that every DOJ information collection subject to the PRA is certified by the Department Clearance Officer prior to transmittal to OMB for approval.

c. The Department CIO, through this program, shall:

(1) Appoint a Department Clearance Officer who shall have independent review authority over component information collections. This authority includes withdrawal, corrective action, or disapproval of the component's information collections. The Department Clearance Officer shall be the only employee granted review and certification authority recognized by OMB. The Department Clearance Officer shall be assigned to the Justice Management Division (JMD) within the DOJ Office of the CIO.

(2) Oversee the PRA program to ensure the proper PRA processes and procedures are followed in managing information collection requests as described in the Department PRA Process and Procedures Guide.

d. The Department Clearance Officer shall:

(1) Manage the DOJ PRA Program to ensure compliance with the requirements of the Act.

(2) Provide strategies and policies for planning and management of the Department's PRA Program.

(3) Review information collection submissions to assure compliance with statutory requirements, OMB guidance, and DOJ policy.

(4) Coordinate the review and validation of information collection data to ensure the accuracy of the Department's annual Information Collection Budget (ICB) compiled by OMB.

(5) Respond, on behalf of the Department of Justice, to inquiries on these matters.

e. Component Heads shall:

(1) Appoint one or more PRA Coordinators to manage component information collection activities, and notify JMD promptly of the name of the appointee(s).

(2) Ensure that information collections in violation of the PRA are reported to the Department Clearance Officer for immediate resolution, and that all component violations are resolved by the end of the current fiscal year.

(3) Ensure that new and existing information collection requests are evaluated to confirm the need for the collections, and that information collections are continually analyzed for methods of reducing burden on the public.

f. Component PRA Coordinators shall:

(1) Manage and maintain a current inventory of component information collections, including identifying information collections that are obsolete, removing them from the inventory, and notifying the Department Clearance Officer within 90-days; and ensure that the Department Clearance Officer has current contact information.

(2) Provide the Department Clearance Officer with the detailed notices to be placed in the Federal Register requesting public comment on proposed information collections, and then resolve comments received.

(3) Review information collection requests for compliance with the PRA and submit the requests in sufficient time to enable the Department Clearance Officer to certify requests before sending them to OMB for approval.

(4) Coordinate information collections with other DOJ components as appropriate.

(5) Determine that the use of the information collection conforms to the requirements of the Privacy Act, the Freedom of Information Act, and any other applicable laws.

(6) Ensure that each information collection has been reviewed and certified by the Department Clearance Officer, approved by OMB, and that it properly displays a valid OMB control number and expiration date (unless waived) prior to undertaking the collection.

(7) Ensure that whenever practicable, information collections shall be conducted electronically.

(8) Submit timely and accurate component annual information collection data for inclusion in the departmental ICB, and validate that information collection requests are consistent with the component's annual ICB submission.

15. INFORMATION QUALITY MANAGEMENT

a. The Information Quality Act, Pub. L. No. 106-554 and the OMB Guidelines for ensuring information quality require federal agencies to ensure the quality, objectivity, utility, and integrity of information disseminated to the public, and establish administrative mechanisms that allow affected persons to seek correction of information that does not comply with the OMB guidance.

b. To satisfy these requirements, the Department has developed DOJ Information Quality Guidelines that require Information Quality Measures to be incorporated into the Department's information dissemination practices, dissemination on DOJ Web sites available to the public, and also dissemination on networks not available to the public.

c. The Department CIO, through these guidelines, shall:

(1) Provide such additional guidance and oversight of information quality procedures as may be needed to ensure compliance with the published OMB and DOJ Information Quality Guidelines throughout the Department and Components.

(2) Establish mechanisms for affected parties to request correction of information that has been or is being disseminated to the public, in accordance with OMB and DOJ Information Quality Guidelines.

d. Component Heads shall:

(1) Designate a component point of contact for information quality and reporting processes.

(2) Ensure awareness of and compliance with the OMB and Department Information Quality Guidelines within their respective component.

(3) Resolve and report the disposition of requests for information correction from the public and peer review results as requested by the Department CIO.

16. INTERNET AND INTRANET SERVICES MANAGEMENT

a. OMB Memo M-05-04, and other supplemental guidance set forth requirements for the use of Federal agency public websites in order to promote a more citizen-centered government. All publicly accessible Department sites shall comply with all privacy laws and guidance, federal accessibility requirements defined in Section 508 of the Rehabilitation Act (Improving Accessibility to Individuals with Disabilities), and Executive Order 13166 (Improving Access to Services for People with Limited English Proficiency), and all laws and guidance relating to Internet Web site security. Additional guidance on recommended policies and guidelines for Department websites is provided at http://dojnet.doj.gov/webdevelopment/index.php and http://dojnet.doj.gov/webdevelopment/guidance.php.

b. For Department Intranet Sites, Section 508 of the Rehabilitation Act and the Freedom of Information Act apply to internal electronic government processes when requests are made by the public for disclosure of information contained on internal agency sites. Disclosure under FOIA is governed by 28 C.F.R. Part 16.

c. For the Department's publicly accessible Internet web sites, the Assistant Attorney General for Administration has established the Department's Web site management program to oversee public access to Department Web content, domain names, and content requirements. The Assistant Attorney General for Administration shall also develop policies and guidance for the Department content hosted on Internet and Intranet Web sites and external hosting providers.

(1) Web Hosting and Publishing Facilities. All Department Internet Web Content shall be hosted on and made available to the public (i.e., published) through Web site hosting services approved by the DOJ CIO.

(2) Domain Names. All Department Internet Web content shall be published under domain names approved and acquired by the DOJ CIO.

(3) Content. The Department and its components shall comply with all relevant laws and guidance, and Department policies, guidance and standards regarding Web content, design and publishing formats, including OMB Memorandum M-05-04 and any other associated guidance. Components shall certify quarterly to the DOJ CIO that all policies and guidance have been met.

(a) The Department and its components shall publish only the following content on the Department's Internet Web sites:

i) Content generated by the Department or another United States government agency.

ii) Content that is in the public domain.

iii) Content for which the Department has obtained written permission from the original source to post on the Department's Internet Web sites. The posting of any such content must include attribution and any appropriate copyright notices.

iv) Content used in accordance with "fair use" principles (*see* 17 U.S.C.§ 107) after consultation with component counsel.

(b) The Department and its components shall, prior to publishing any content on the Department's Internet Web sites, submit such content for review and approval by the appropriate Component Web Content Authorizer or his designee (whose responsibilities are described below), who must be employees of the Department.

(4) Records: Records must be kept in compliance with all National Archives and Records Administration (NARA) regulations. Information that is a federal record should be managed and retained in accordance with the department's Records Management policies and the applicable records schedule approved by NARA. For further information and guidance regarding record keeping practices for websites, see http://www.archives.gov/records-mgmt/initiatives/web-tech.html.

d. The Department CIO, through this program, shall:

(1) Deploy, operate, and maintain the information technology resources used to host the Department's Internet Web Sites.

(2) Oversee the operation of the Department's Internet Web sites to ensure that they comply with information technology statutes, regulations, policies, and guidance.

(3) Review component requests for component-specific domain names and hosting services.

(4) Designate the Department Web Content Manager.

e. The Department Web Content Manager shall:

(1) Ensure that content on the Department's Internet Web sites that is not affiliated with a specific DOJ component is in compliance with relevant Federal laws and guidance, as well as Department policies, guidance, and standards regarding Web content.

(2) Work with Component Web Content Authorizers and Managers to ensure that the content on their component Web pages and sites is in compliance with relevant Federal laws and guidance as well as Department policies, guidance and standards regarding Web content.

(3) Obtain review and approval by the Component Head for content, including hyperlinks that may be inconsistent with the Department's mission, policy or initiatives.

f. Component Heads shall:

(1) Oversee all component decisions on content appropriateness.

(2) Appoint Component Web Content Managers and Component Web Content Authorizers and inform the Department's Web Content Manager of such Appointments.

g. Component Content Managers shall:

(1) Ensure that the operation of their component Websites complies with relevant information technology laws, policies, and guidance.

(2) Submit requests for approval of component-specific hosting services and Domain names to the Department CIO.

(3) Ensure that the content on component Web pages and sites is appropriate.

(4) Establish procedures for publishing content on their component Web pages.

(5) Maintain FOIA pages for their component Web pages and sites and ensure that these pages include the required information and records.

h. The Component Web Content Authorizer shall:

Ensure that the content on Component Web pages and sites is in compliance with relevant Federal laws and guidance as well as Department policies, guidance, and standards regarding Web content by reviewing and approving all content prior to publication. For further guidance on the responsibilities of the Web Content Authorizer see Department of Justice Guidance for the Implementation of OMB Policies for Federal Agency Web Sites.

17. ELECTRONIC RECORDS AND INFORMATION MANAGEMENT

a. The Federal Records Act, 44 U.S.C. § 3101, and implementing regulations define federal records and require that Executive Agencies manage their records to facilitate appropriate preservation, retrieval, use, and disposition.

b. Order DOJ 2710.11 sets forth the Department's policy for management of records in accordance with these statutory and regulatory requirements, regardless of format. The Order also establishes that the Office of Records Management Policy (ORMP) is responsible for records management business policy, direction, guidance, and development of business requirements for the management of electronic records.

c. The Department CIO shall:

(1) Develop, in coordination with ORMP and through the ERM and appropriate work groups, IT standards and guidance to implement the statutory requirements of the Federal Records Act and other applicable regulatory and policy requirements for electronic Records and Information Management.

(2) Establish processes for reviewing Department records and information management systems to ensure compliance with applicable federal laws, regulations and policies.

(3) Provide capabilities for appropriately managing and preserving records for the Department's senior leadership and management offices consistent with applicable federal laws, regulations and policies.

d. Component Heads shall:

(1) Ensure that appropriate records and information management processes and capabilities are implemented to comply with the Department's records management policies as defined in Order DOJ 2710.11, and any additional Department guidance, and applicable federal laws, regulations, and policy.

(2) Develop and publish such additional guidance as may be necessary to ensure consistent records and information management processes and practices are implemented within the component.

APPENDIX 1. DEFINITIONS.

Component refers to the DOJ bureaus, offices, boards, and divisions.

Computer system is a discrete set of electronic information resources (data, hardware and software) organized for the collection, processing, maintenance, transmission, and dissemination of information.

Continuity of Operations (COOP) Plan is a document that establishes policies and procedures to provide for the continuance of critical IRM operations, that will ensure the continued performance of Departmental and component essential functions during any emergency or situation that may disrupt normal operations. The COOP Plan must be in compliance with the Federal Emergency Management Agency's Federal Circular 65 and Order DOJ 2640.2F.

Electronic Record has the meaning given in 44 U.S.C. § 3301 meaning any information recorded in a form that only a computer can process and that satisfies the definition of a Federal record, and information technology records. Electronic Records are copies of records that are created on electronic and word processing systems and used solely to generate a record keeping copy of the records found in the General Records Schedule 27. Electronic Records also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination

Employee with Disabilities means an employee has a physical or mental impairment that substantially limits one or more major life activities or has a record of such impairment or is regarded as having such impairment. In general, this includes individuals with a significant vision, hearing, dexterity, cognitive or mobility impairment.

Enterprise Architecture (EA) is an integrated agency-wide blueprint that explains and guides how an organization's IT and information management elements work together to accomplish the mission of the organization. An EA addresses the following views: business activities and processes, data sets and information flows, applications and software, and technology. An EA includes a current (baseline) architecture, desired (target) architecture, and a sequencing plan.

Information Resources has the meaning given in 44 U.S.C §3502(6), i.e., information and related resources, such as personnel, equipment, funds, and information technology.

Information Technology (IT) has the meaning given in Section 5002(3) of the Clinger-Cohen Act of 1996, i.e., any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. As further clarified in OMB Circular A-11, IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

IT Administration Records are records accumulated by individual offices that relate to the internal administration or housekeeping activities of the office rather than the functions for which the office exists.

IT Contingency Plan (ITCP) documents and maintains a plan for the continuity of general support systems and contingency plans for major applications. NIST Publication 800-34 considers continuity of support planning to be synonymous with IT contingency planning. OMB Circular A-130, Appendix III, and ITSS Standard 2.4 require the development and maintenance of ITCP's for every IT system and application. The general definition of the contingency plan is: "a plan used by an organization or business unit to respond to a specific systems failure or disruption of operations. A contingency plan may use any number of resources including workaround procedures, an alternate work area, a reciprocal agreement, or replacement resources."

IT Investment is the expenditure of resources on selected IT, or IT-related initiatives with the expectation that the benefits will exceed the value of the resources expended.

IT Investment Plan identifies the investments (for projects and programs) sought to implement the EA and specifies the priority of the investments in relation to mission criticality and management visibility, as well as information concerning investment sequencing and other dependencies to guide planners during project selection.

IT Investment Portfolio is the combination of all IT assets, resources, and investments owned or planned by an organization in order to achieve its strategic goals, objectives, and mission.

IT Project is an organizational initiative that employs or produces IT or IT related assets. Each project has or will incur costs, expects or will realize benefits, has a schedule of project activities and deadlines, and has or will incur risks.

IT Project Manager is the person who manages day-to-day project activities. In the case where an investment is for one project, the IT project and investment managers are one and the same. In the case where an investment is for multiple projects, the IT project manager and investment project manager may be different people.

IT Records are the data or information content of an information technology system.

IT systems provide a service, such as a software system, used to create, store, access and/or retrieve data stored in a data base.

Internet is the publicly available worldwide network of computer systems, services and electronic media, interconnected through the Transmission Control Protocol/Internet Protocol, and related protocols.

Intranet is any private, or limited access network of computer systems, services and electronic media, interconnected through the Transmission Control Protocol/Internet Protocol, and related protocols.

Logical Entity Exchange Specification (LEXS) is a standard framework for building NIEM-conformant information exchange packages used by DOJ in various law enforcement information sharing applications. In particular, LEXS specifies how law enforcement information should be packaged and delivered to information sharing applications. LEXS also specifies how partner applications can perform federated searches to access distributed information from across many sources. More information on LEXS can be found at www.LEXS.gov.

Major IT Investment as defined in OMB Circular A-11, is a system or investment that requires special management attention because of its importance to an agency's mission; investment was a major investment in the prior year's budget submission and is continuing; investment is for financial management and spends more than $500,000; investment is directly tied to the top two layers of the Federal Enterprise Architecture (Services to Citizens and Mode of Delivery); investment is an integral part of the agency's modernization blueprint (EA); investment has significant program or policy implications; investment has high executive visibility; or investment is defined as major by the agency's capital planning and investment control process. Investments that are E-Government in nature or use e-business technologies must be identified as major investments regardless of the costs. Systems not considered "major" are "non-major."

National Information Exchange Model (NIEM) is a standard data model consisting of the commonly defined data dictionary, formal naming and design rules for extending the model, and standardized specifications and processes for building and documenting information exchanges using eXtensible Markup Language (XML). NIEM is used to share information within the Department, among federal agencies, and between agencies at all levels of government: Federal, state, local and tribal. More information on NIEM can be found at www.NIEM.gov.

Systems Development Life Cycle (SDLC) is a methodology which establishes procedures, practices, and guidelines for the management of a single investment program. It governs how DOJ information systems shall be planned, developed, implemented, and managed until disposal.

APPENDIX 2. REFERENCES.

FEDERAL LAWS AND CONGRESSIONAL MANDATES.

18 U.S.C. § 1913 (lobbying with appropriated moneys).

Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6506.

Clinger Cohen Act of 1996, 40 U.S.C. § 1425.

Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030.

Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552(a).

Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002).

Electronic Communications Privacy Act of 1986, 25 U.S.C. §§ 2510-2521.

Electronic Signatures in Global and National Commerce Act (E-SIGN Act), 15 U.S.C. § 7001.

Federal Acquisition Streamlining Act of 1994, Pub. L. No. 103-355, 108 Stat. 3243 (1994).

Federal Funding Accountability and Transparency Act of 2006

Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107-347, 116 Stat. 2899, (2002). (This is a component of the E-Government Act, cited above.)

Federal Managers Financial Integrity Act of 1982, Pub. L. No. 97-255 (1982).

Federal Records Act, 44 U.S.C. § 3301

Federal Reports Act of 1942, 44 U.S.C. §§ 3501-3511.

Freedom of Information Act (FOIA), 5 U.S.C. § 552.

Government Paperwork Elimination Act of 1998 (GPEA), 44 U.S.C. § 3504.

Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62, 107 Stat. 285 (1993).

The Intelligence Reform and Terrorism Prevention Act of 2004

Notification and Federal Employee Anti-discrimination and Retaliation Act of 2002 (No FEAR Act) Pub. L. No. 107-174, 116 Stat. 566 (2002).

Paperwork Reduction Act of 1995, 44 U.S.C. §§ 3501-3520.

Privacy Act of 1974 (as amended by the Computer Matching and Privacy Protection Act of 1988), 5 U.S.C. § 552.

Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

Treasury and General Government Appropriations Act for Fiscal Year 2001, Pub. L. No. 106-554, 114 Stat. 2763 (2001).

Treasury, Postal Service and General Government Appropriations Act, Pub. L. No. 101-136 (1990).

Workforce Investment Act of 1998, 29 U.S.C. § 794d (Section 508 of the Rehabilitation Act of 1973), as amended.

PRESIDENTIAL EXECUTIVE ORDERS AND OFFICE OF MANAGEMENT AND BUDGET (OMB) GUIDANCE.

Executive Memorandum, Electronic Government, June 12, 1999.

Executive Memorandum, Expanding Access to Internet-based Educational Resources for Children, Teachers, and Parents, April 18, 1997.

Executive Memorandum, Plain Language in Government Writing, June 1, 1998.

Exec. Order 12,861, 3 C.F.R. 630 (1993).

Exec. Order 12,866, 58 Fed. Reg. 51,735 (Sept. 30, 1993).

Exec. Order 13,166, 65 Fed. Reg. 50123 (Aug. 11, 2000).

Executive Order 13388, 70 FR 62023, October 27, 2005

http://www.archives.gov/federal-register/executive-orders/2005.html

Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818 (June 16, 1989).

OIRA Memorandum from John D. Graham and Karen S. Evans to the President's Management Council on "Regulations.Gov"(March 1, 2004).

OMB Annual Bulletin: Information Collection Budget (ICB) Agency Implementation Guidance.

OMB Circular A-11, Preparation, Submission and Execution of the Budget

OMB Circular A-109, Major System Acquisitions. Subpart 34

OMB Circular A-130, Management of Federal Information Resources (with Appendices and periodic revisions).

OMB E-Government Strategy, April 2003

OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies; Notice; Republication (Information Quality Guidelines), 67 Fed. Reg. 369-378 (January 3, 2002), corrected, 67 Fed. Reg. 5365 (February 5, 2002).

OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites (June 2, 1999).

OMB Memorandum M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act (April 25, 2000).

OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites (June 22, 2000).

OMB Memorandum M-00-15, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act (September 25, 2000).

OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy (December 20, 2000).

OMB Memorandum M-03-18 Implementation Guidance for the E-Government Act of 2002 (August 1, 2003).

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003).

OMB Memorandum M-04-08, Maximizing Use of SmartBuy and Avoiding Duplication of Agency Activities with the President's 24 E-Gov Initiatives (February 25, 2004).

Privacy Act Implementation, Guidelines and Responsibilities, 40 Fed. Reg. 28948 (July 9, 1975).

FEDERAL/DEPARTMENTAL REGULATIONS/GUIDANCE.

Architectural and Transportation Barriers Compliance Board (Access Board) Standard, 36 C.F.R. 1194.

Controlling Paperwork Burdens on the Public, 5 C.F.R. 1320.

Order DOJ 2400.3, Justice Property Management Regulation.

Order DOJ 2640.1, Privacy Act Security Regulations for Systems of Records.

Order DOJ 2640.2E, Information Technology Security.

DOJ Graphic Standards Manual, published by the JMD Facilities Services Staff.

Electronic and Information Technology Accessibility Standards, 36 C.F.R. 1194.

Federal Acquisition Regulation, 48 C.F.R. 1.

Federal Management Regulation, 41 C.F.R. 102-173.

FOIA Update, Vol. XIX, No. 3, at 3-4 ("OIP Guidance: Recommendations for FOIA Web Sites").

Justice Acquisition Regulations, 48 C.F.R. 28.

NARA Regulations, 36 C.F.R. 1220-1238.

Personal Use of Government Property, 28 C.F.R. 45.4.

Telecommunications Management Policy, 41 C.F.R. 101-35.