U.S. Department of Justice **0903**

Approved On: MAY 0 5 2016

DOJ Order

INFORMATION TECHNOLOGY MANAGEMENT

PURPOSE:	Establishes Department of Justice (DOJ) policy for enterprise information technology (IT) management
SCOPE:	All Department components
ORIGINATOR:	Justice Management Division, Office of the Chief Information Officer
CATEGORY:	(I) Administrative, (II) Information Technology
AUTHORITY:	See Appendix A
CANCELLATION:	Order DOJ 2880.1C: Chapter 1; Chapter 2, Section 1 – "IT Strategic Planning," Section 2 – "Information Sharing," Section 3 – "IT Enterprise Architecture," Section 4 – "IT Performance Management," Section 5 – "IT Investment Management," Section 6 – "IT Program and Project Management," Section 7 – "IT Oversight Management," Section 8 – "IT Acquisition Management," Section 9 – "IT Accessibility," Section 10 – "IT Security Management," Section 11 – "IT Infrastructure and Asset Management," Section 12 – "IT Workforce Management," Section 13 – "Protection and Privacy of Personally Identifiable Information," Section 14 – "Information Collection Management," Section 15 – "Information Quality Management," Section 17 – "Electronic Records and Information Management"; DOJ Memo 2016-03, Major Information Technology Investment Risk Management and TechStat Reporting
DISTRIBUTION:	Electronically distributed to those referenced in the "SCOPE" section and posted to the DOJ directives electronic repository (SharePoint)

APPROVED BY: *Lee J. Lofthus*
Assistant Attorney General for Administration

ACTION LOG

All DOJ directives are reviewed, at minimum, every 5 years and revisions are made as necessary. The action log records dates of approval, recertification, and cancellation, as well as major and minor revisions to this directive. A brief summary of all revisions will be noted. In the event this directive is cancelled, superseded, or supersedes another directive, that will also be noted in the action log.

Action	Authorized by	Date	Summary
Initial Document Approval	Lee J. Lofthus Assistant Attorney General for Administration	MAY 0 5 2016	Establishes DOJ policy for the procurement, use, governance, and management of enterprise IT resources.

TABLE OF CONTENTS

DEFINITIONS

Term	Definition
Accessibility (or Accessible)	The design of products, devices, services, or environments for people with disabilities. Accessible design ensures both "direct access" (i.e., unassisted) and "indirect access," meaning compatibility with an individual's assistive technology (e.g., computer screen readers).
Capital Planning and Investment Control	An integrated process within an agency for planning, budgeting, procuring, and managing the agency's portfolio of capital assets to achieve the agency's strategic goals and objectives with the lowest overall cost and least risk.
Component Chief Information Officer	The person within the component accountable for information technology (IT) management as defined in this policy statement. In components that do not have a designated component Chief Information Officer (CIO) position, this role may apply to IT Directors who are responsible for IT management within the component. Components that rely entirely on the Justice Management Division for IT management and services are not required to have an individual in this role.
Electronic and Information Technology	Any IT, equipment, or interconnected system or subsystem of equipment for which the principal function is the creation, conversion, duplication, automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, reception, or broadcast of data or information. Examples of electronic and information technology include, but are not limited to, electronic content (websites, digital files, and electronic documents); software and applications (e.g., Sentinel, Palantir); IT services; telecommunications products (telephones, VOIP systems, videophones, and smartphones); computers and ancillary equipment (desktops, laptops, tablets, and peripherals); information kiosks and transaction machines (e.g., the Federal Bureau of Investigation Wall of Honor kiosk); videos and multimedia content, including webcasts; office equipment (e.g., printers, copiers, scanners and fax machines); and assistive technology and software.
Enterprise	Synonymous with Department-wide.
Enterprise Architecture	The process of translating business vision and strategy into effective enterprise change by creating, communicating, and improving the key requirements, principles, and models that describe the future state of the enterprise and enable its evolution.
External Partners	Mission partners and stakeholders outside the Department of Justice (DOJ), such as other federal agencies; state, local, tribal, territorial, and international governments; private industry; grant organizations; and academia.

Term	Definition
Information Technology	Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.
IT Information Management	IT practices centered on the management of DOJ information. This includes all IT practices needed to manage electronic information throughout its life-cycle, from capture/creation, to final disposition, for the purpose of sharing and protecting the information.
IT Investment	The expenditure for IT resources required to accomplish mission objectives. An IT investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or group of IT assets with related functionality and the subsequent operation of those assets in a production environment.
IT Project	A temporary endeavor undertaken to build or acquire a unique product or service with a defined start and end point and specific objectives that, when attained, signify completion. Projects are undertaken for development, modernization, enhancement, disposal, or maintenance of an IT asset. Projects are composed of activities.
Major IT Investment	An IT investment that requires special management attention because of its; (1) importance to the mission or function of the government; (2) significant program or policy implications; (3) high executive visibility; (4) high development, operating, or maintenance costs; (5) unusual funding mechanism; or (6) designation as major by the DOJ CIO as described in the capital planning and investment control process.
Oversight Manager	Oversees the activities of an IT management function, but may not manage the day-to-day activities of the function. The DOJ Oversight Manager oversees activities enterprise-wide, across components. The component Oversight Manager (OM) oversees activities within the component. The DOJ and component OMs work together to develop standards and procedures (S&Ps) for the function and monitor the performance of the function and compliance with the S&Ps.
TechStat Session (or TechStat)	A face-to-face, evidence-based accountability review of a major IT investment conducted by the Department Investment Review Council (DIRC). TechStat sessions are a tool used for identifying or anticipating critical problems in an investment, turning around underperforming investments, pausing or re-scoping projects to reduce risk, or terminating investments, if appropriate.

Term	Definition
TechStat Session Scheduling Requirements	The Office of Management and Budget (OMB) requires that a TechStat session be scheduled for major IT investments that are identified as underperforming for 3 consecutive months. TechStat sessions are performed by the DIRC, and scheduled by the DOJ CIO. OMB requires that the session be scheduled before the investment reaches 4 consecutive months of underperformance and requires notification of the session 2 weeks in advance. The DOJ CIO has the discretion to schedule the TechStat session sooner, as deemed appropriate.
TechStat Session Review Requirements	A TechStat session must identify the root causes of the high risk(s), the extent to which the risk(s) can be addressed, and the probability of future program success.
Underperforming Major IT Investment	A major IT investment for a development, modernization, or enhancement project with a greater than 10% variance from meeting its schedule, cost, or performance targets.

ACRONYMS

Acronym	Meaning
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DAAG/CIO	Deputy Assistant Attorney General/Chief Information Officer
DIRB	DOJ Investment Review Board
DIRC	DOJ Investment Review Council
DOJ	Department of Justice
EA	Enterprise Architecture
eCPIC	Electronic Capital Planning and Investment Control
ITIL	Information Technology Infrastructure Library
IT	Information Technology
JMD	Justice Management Division
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget

Acronym	Meaning
PRA	Paperwork Reduction Act
S&Ps	Standards and procedures
SAVE Council	Attorney General's Advisory Council for Savings and Efficiencies

I. Policy

It is the policy of the Department of Justice (DOJ or Department) that the Department and its components plan, acquire, manage, and use information technology (IT) and information in a secure manner that enhances mission accomplishment, improves work processes and employee productivity, provides sufficient protection for the privacy of personal information, promotes citizen-centered electronic government, and complies with all applicable federal laws and directives.

II. Roles and Responsibilities

A. Department Information Technology Leadership

1. The DOJ Chief Information Officer (CIO) is appointed by the Attorney General.

2. The Department Investment Review Board (DIRB), chaired by the Deputy Attorney General, ensures that taxpayer funds are optimally spent.

3. The Assistant Attorney General for Administration must hire the DOJ Chief Information Officer (CIO) to head the Office of the CIO (OCIO).

4. The Deputy Assistant Attorney General for Information Resources Management/DOJ Chief Information Officer must:

    a. Provide leadership and accountability for IT management, governance, and oversight processes across the enterprise.

    b. Advise Department leadership on all matters pertaining to IT.

    c. Develop and implement enterprise IT policy pursuant to the authorities and responsibilities set forth in this Order, and, where practical, in consultation with the DOJ CIO Council. Except where otherwise authorized by law, regulation, or other policy, the DOJ CIO has the authority to set enterprise IT policy, standards, procedures, and guidance in order to ensure sound management practices in all areas of IT governance, as described in this Order.

    d. Concur upon the hiring of component CIOs and engage in the evaluation of their performance.

    e. Participate in the functions of the Federal Chief Information Officers Council, chaired by the Federal CIO.

    f. Serve as Vice-chair for the DIRB.

g. Serve as Chair for the DOJ Investment Review Council (DIRC).

h. Serve as the component CIO for the Justice Management Division (JMD). The responsibilities for the JMD CIO are the same as defined for all component CIOs, with one addition – the JMD CIO is responsible for supporting the preservation activities of the JMD senior leadership offices.

5. The DOJ Controller must:

a. Ensure that IT investments, through the capital planning and investment control process, are integrated into the DOJ budget formulation and execution processes.

b. Serve as a member of the DIRB and as vice-chair of the DIRC to provide financial oversight.

c. Verify/certify/ensure that the DOJ CIO approves funding associated with IT investments in the Department's annual and multi-year planning, programming, budgeting, and executing processes.

d. Verify/certify/ensure that the DOJ CIO approves all IT requests for reprogram funding.

6. The DOJ Senior Procurement Executive must:

a. Ensure that IT acquisitions are appropriately integrated into the enterprise acquisition processes.

b. Assist with the development and management of enterprise-wide IT contracts to be consistent with federal strategic sourcing initiatives and ensure their use to the maximum extent possible.

c. Ensure that all IT acquisitions are made with DOJ CIO approval and/or in accordance with DOJ CIO-approved IT acquisition procedures.

7. The DOJ Chief Human Capital Officer must:

a. Establish enterprise human resource processes that enable evaluation of the knowledge and skills of the enterprise IT workforce to determine its adequacy or the need for corrective action.

b. Ensure, through dissemination of policy, that component Human Resources Offices: (1) are aware that the DOJ CIO must concur upon the appointment of a component CIO, (2) incorporate enterprise critical element(s) into

component CIO performance work plans, and (3) provide the DOJ CIO with the opportunity to contribute to the performance reviews of component CIOs.

c. Develop and maintain a directory of component CIOs.

8. The Senior Agency Official for Privacy must conduct privacy compliance reviews.

9. The DOJ Inspector General is responsible for conducting Federal Information Security Management Act of 2002 (FISMA) audits.

B. Component Information Technology Leadership

1. The Head of Component must:

a. Engage the DOJ CIO when hiring and appointing a component CIO and submit names of nominees to the DOJ CIO for concurrence.

b. Ensure that approved performance evaluation criteria are incorporated into the component CIO's performance plan and that the rating official discusses the DOJ CIO's performance input provided for the component CIO's regular reviews and final ratings.

c. Ensure that the component CIO has regular access to the Head of Component on IT matters.

d. Ensure that the DOJ CIO is informed of all technology spending that is not under the DOJ CIO's direct control.

2. The component Chief Information Officer must:

a. Provide leadership and accountability for IT acquisition, management, governance, and oversight processes across the component.

b. Advise the Head of Component and DOJ CIO on all IT-related matters within their component, through chain of command, as appropriate.

c. Support the enterprise IT goals laid out in the DOJ IT Strategic Plan and the evaluation criteria identified in the enterprise critical element(s).

d. Participate in the leadership and management of DOJ IT resources through appropriate governing bodies.

e. Ensure that assets placed onto the component and DOJ networks are secure, properly maintained, and aligned with enterprise architecture (EA), to ensure consistency across the Department.

f. Implement all component CIO provisions of this Order.

C. Information Technology Executive Boards and Councils

1. The Department Investment Review Board must:

   a. Provide executive-level oversight (monitoring costs, schedules, performance, and risks) of DOJ's most critical IT investments to ensure disciplined selection, management, and return on investments. This oversight is supported by the DIRC.

   b. Review, validate, and approve investments that meet established criteria, including the review and validation of portfolio placement and alignment with DOJ's strategic mission.

2. The Department Investment Review Council must:

   a. Provide investment oversight (monitoring costs, schedules, performance, and risk) of DOJ's major IT investments to ensure disciplined selection, management, and return on investment.

   b. Conduct TechStat reviews of underperforming major IT investments. Address TechStat Session Review Requirements during the reviews. Specify corrective actions with timelines for improving performance and reducing risk, or pause, re-scope, or terminate the investment, as appropriate.

3. The DOJ CIO Council is an advisory group to the DOJ CIO and must:

   a. Advise the DOJ CIO on all matters related to IT and actively participate in the formulation and implementation of IT strategies, procedures, and practices.

   b. Support the DOJ CIO, either directly or through committees and working groups that may be established, as needed. These committees and working groups may be permanent or temporary and must be chaired by a CIO Council member.

D. Information Technology Strategy Oversight

The DOJ CIO and component CIO must:

DOJ CIO	Component CIO
1. IT Strategy. Develop and implement an enterprise-wide IT Strategic Plan that supports DOJ's mission and goals, drives investment decisions, and monitors progress toward achieving its goals.	1. Advise the DOJ CIO on the development of DOJ's enterprise IT Strategic Plan, implements the strategic goals in the component, and report progress and performance to the DOJ CIO.
2. Component Alignment. Ensure that component IT strategic plans demonstrate alignment with DOJ's IT strategic plan.	2. Align component IT strategic plans, if produced, with the DOJ IT strategic plan.
3. DOJ CIO Council. Establish a governance council, referred to as the DOJ CIO Council, to enable component CIOs to participate in executive level strategic decisions and enterprise oversight.	3. Participate in the DOJ CIO Council, engage in executive level strategic decisions, and provide enterprise oversight.
4. IT Marketplace. Monitor the state of enterprise-wide IT at given points in time, evaluate trends, stay abreast of emerging technologies, and implement improvements.	4. Report to DOJ CIO on the state of IT in the component at given points in time and evaluate trends.
5. Designee. Designate a DOJ IT Strategy Oversight Manager to act on behalf of the DOJ CIO to oversee enterprise IT strategic management across the Department, as defined in the Information Technology Strategy Oversight Policy Statement.	5. Designate a component IT Strategy Oversight Manager to coordinate with DOJ IT Strategy Oversight Manager on behalf of the component CIO on matters concerning enterprise IT strategic management and to oversee strategic management within the component, as defined in the Information Technology Strategy Oversight Policy Statement.

Click on Information Technology Strategy Oversight to see the Policy Statement.

E. Information Technology Investment Oversight

The DOJ CIO and component CIO must:

DOJ CIO	Component CIO
1. Taxpayer Funds Stewardship. Foster an enterprise culture that encourages cost savings and avoidance. Establish integrated enterprise and component investment management processes and governance that promote wise stewardship of taxpayer funds.	1. Foster a component culture that encourages cost savings and avoidance. Integrate component processes for investment management and governance with processes across the enterprise.

DOJ CIO	Component CIO
2. OMB Business Case Requirements. Integrate Office of Management and Budget (OMB) requirements for investment business cases and the IT portfolio summary with the DOJ budget formulation process.	2. Ensure that component IT budgets and expenditures wisely manage taxpayer funds and are aligned with IT enterprise goals.
3. Council Support. Support the Attorney General's Advisory Council for Savings and Efficiencies (SAVE Council).	3. Support the Attorney General's SAVE Council.
4. Investment Performance. Ensure that components monitor performance of major IT investments and identify underperforming major IT investments per DOJ policy. Schedule, and conduct TechStat sessions for DIRC review of underperforming major IT investments, and address OMB requirements for scheduling, follow-through, and reporting.	4. Monitor all component IT investment performance through regular reviews and engagement with the program sponsor and stakeholders, identify underperforming major IT investments and report to the DOJ CIO, support DIRC TechStat sessions, and implement corrective actions.
4.1. Participate in component reviews of IT major investments or designate an executive representative to participate, as appropriate.	4.1. Conduct reviews of component underperforming major IT investments through established component governance bodies. Include the DOJ CIO, or designated representative, as members and invite them to participate.
4.2. Refer underperforming major IT investments to the DIRC for TechStat review, ensuring that TechStat Session Scheduling Requirements are met. As chair, ensure that the DIRC addresses the TechStat Session Review Requirements.	4.2. Deliver timely and accurate reports on component major IT investments to the DOJ CIO as specified in DOJ policy and procedures. For underperforming major IT investments, include decisions for reducing risks.
4.3. Monitor underperforming investments for improvement or termination.	4.3. Improve component underperforming major IT investments or terminate them, as appropriate.
4.4. Notify the DIRB when the DIRC determines that a major investment should be paused, re-scoped, or terminated.	
4.5. Ensure that accurate cost, schedule, risk, and performance data for all Department major IT investments are made available to the public in a timely manner, per OMB guidance.	

DOJ CIO	Component CIO
5. Project Management Practices. Establish IT project management practices that promote standard development life cycles for enterprise and component use. Ensure that reporting and security requirements relevant to IT project managers are easily accessible and highlight required actions.	5. Implement project management practices within the component that comply with DOJ standards, procedures, and guidance. Ensure that component project managers are appropriately certified.
6. Project Manager Qualifications. Ensure that Component IT project managers are certified and qualified.	6. Designate component IT project managers to run projects and programs. Ensure project managers maintain current certification and adhere to policy, as defined in the Information Technology Investment Oversight Policy Statement.
7. Designee. Designate a DOJ IT Investment Oversight Manager to act on behalf of the DOJ CIO to oversee enterprise IT investment management across the Department, as defined in the Information Technology Investment Oversight Policy Statement.	7. Designate a component IT Investment Oversight Manager to coordinate with DOJ IT Investment Oversight Manager on behalf of the component CIO on matters concerning enterprise IT investment management and to oversee investment management within the component, as defined in the Information Technology Investment Oversight Policy Statement.

Click on Information Technology Investment Oversight to see the Policy Statement.

F. Information Technology Acquisition Oversight

The DOJ CIO and component CIO must:

DOJ CIO	Component CIO
1. Acquisition Processing. Establish enterprise processes and practices for all IT acquisitions that are integrated with DOJ procurement policies, green purchasing requirements, and requirements for assurance of non-duplication of Administration e-government initiatives.	1. Follow enterprise practices for IT acquisitions and provide accurate and timely reporting to the DOJ CIO for all component IT acquisitions, even those that do not require DOJ CIO approval, in order to provide enterprise visibility of IT acquisitions.
2. Acquisition Plan Review. Review and approve IT acquisition plans, strategies, and procurements. Delegate approval authority, as appropriate.	2. Submit for approval the component's IT acquisitions proposals that require the DOJ CIO's approval. Approve the component's other IT acquisitions through delegated authority from the DOJ CIO.

DOJ CIO	Component CIO
3. Government-wide Contract Agreements. Promote the use of government-wide and enterprise contracting vehicles across the enterprise. Ensure contracts are efficient and cost effective. Approve new agency-wide IT contracts and delegate authority, as appropriate, to component CIOs to enter into agreement with vendors through their contracting officers for IT products and services.	3. Promote the use of government-wide and enterprise contracting vehicles and strategic sourcing within the component. Ensure contracts are efficient and cost effective. Ensure use of enterprise IT contracts, when appropriate. Through delegated authority from the DOJ CIO, and through component contracting officers, enter into agreements with vendors directly to acquire products and services not available through enterprise or other blanket purchase agreements.
4. Designee. Designate a DOJ IT Acquisition Oversight Manager to act on behalf of the DOJ CIO to oversee enterprise IT acquisition management across the Department, as defined in the Information Technology Acquisition Oversight Policy Statement.	4. Designate a component IT Acquisition Oversight Manager to coordinate with the DOJ IT Acquisition Oversight Manager on behalf of the component CIO on matters concerning enterprise acquisition management and oversee acquisition as defined in the Information Technology Acquisition Oversight Policy Statement.

Click on Information Technology Acquisition Oversight to see the Policy Statement.

G. Information Technology Workforce Oversight

The DOJ CIO and component CIO must:

DOJ CIO	Component CIO
1. Equipped Workforce. Ensure that the DOJ IT workforce is skilled and equipped to perform the work needed to maintain the current state of IT and is positioned to perform the work needed to achieve IT strategic goals.	1. Advise the DOJ CIO on the development of strategic goals and plans for promoting a skilled and equipped workforce. Implement the plans within the component.
2. Grow Skill Base. Assess IT workforce skills and competencies and determine gaps and areas for improvement. Develop and implement recruitment strategies to attract and hire the most qualified and competitive IT talent.	2. Assist the DOJ CIO with determining gaps in workforce skills and developing recruitment strategies.
3. Culture of Engagement. Build an enterprise culture of engagement that promotes the exploration of new technologies, standards, and processes and rewards innovation.	3. Build a component culture of engagement that promotes the exploration of new technologies, standards, and processes and rewards innovation.

DOJ CIO	Component CIO
4. Component CIO Hiring. Work with the DOJ Chief Human Capital Officer to participate in the process for hiring component CIOs, concur upon the appointment of a component CIO, and create appropriate Performance Work Plan language for General Schedule and Senior Executive Service component CIOs. Provide input to the component CIO rating officials in a timely manner for inclusion in regular appraisals.	4. Work with the component Human Resources Office to ensure that the DOJ CIO is engaged in the annual drafting of the component CIO Performance Work Plans and subsequent performance reviews.
5. Designee. Designate a DOJ IT Workforce Oversight Manager to act on behalf of the DOJ CIO to oversee enterprise IT workforce management across the Department, as defined in the Information Technology Workforce Oversight Policy Statement.	5. Designate a component IT Workforce Oversight Manager to coordinate with the DOJ IT Workforce Oversight Manager on behalf of the component CIO, to oversee IT workforce management within the component, as defined in the Information Technology Workforce Oversight Policy Statement.

Click on Information Technology Workforce Oversight to see the Policy Statement.

H. Information Technology Enterprise Architecture Oversight

The DOJ CIO and component CIO must:

DOJ CIO	Component CIO
1. Federal Alignment. Develop and maintain an EA that is aligned with the federal EA and align the Department's IT investments with the EA.	1. Assist the DOJ CIO in the development of an EA, develop supportive component target architectures, and align the component's IT investments with the EA.
2. EA Reviews. Develop and implement guidance and procedures for EA reviews of all IT investments and conduct EA reviews of major investments.	2. Conduct EA reviews of component IT investments.
3. Designee. Designate a DOJ IT Enterprise Architecture Oversight Manager to act on behalf of the DOJ CIO to oversee IT enterprise architecture management across the Department, as defined in the Information Technology Enterprise Architecture Oversight Policy Statement.	3. Designate a component IT Enterprise Architecture Oversight Manager to coordinate with the DOJ IT Enterprise Architecture Oversight Manager on behalf of the component CIO to oversee IT enterprise architecture management within the component, as defined in the Information Technology Enterprise Architecture Oversight Policy Statement.

Click on Information Technology Enterprise Architecture Oversight to see the Policy Statement.

I. Information Technology Information Oversight

The DOJ CIO and component CIO must:

DOJ CIO	Component CIO
1. Internal Sharing. Develop and implement strategies for managing enterprise data and information. Promote information sharing, as appropriate, throughout the enterprise and with external partners.	1. Assist the DOJ CIO with developing and implementing strategies for enterprise data and information. Promote information sharing, as appropriate, throughout the enterprise and with external partners and implement strategies within the component.
2. External Sharing. Lead and coordinate information sharing between key federal agencies, between federal agencies and state and local law enforcement and judicial agencies, and between the United States and foreign partners.	2. Assist the DOJ CIO with coordinating information sharing activities with external entities.
3. Sharing Standards. Build an information sharing reference architecture. Adopt consistent technical exchange standards and open community standards, wherever possible, to support content sharing between communities (both DOJ components and external partners) and applications. Leverage the National Information Exchange Model, Law Enforcement Information Sharing Program Exchange Specifications, and Open Geospatial Consortium for law enforcement.	3. Partner with the DOJ CIO to build an information sharing architecture and technical exchange standards and implement them within the component.
4. Data Marketing. Bring components together to maximize the use of existing DOJ data and identify new sources and new uses for data.	4. Partner with the DOJ CIO to maximize the use of existing DOJ data and identify new sources and new uses for data.
5. Governance and Financial Data. Share data captured through governing and financial processes with stakeholders, when appropriate, to improve transparency and foster stronger relationships.	5. Share data captured through governing and financial processes with the DOJ CIO for aggregation and distribution to improve transparency and foster stronger relationships.
6. Downstream Sharing. Ensure that information is created across the enterprise in a manner that supports downstream information processing and dissemination when possible.	6. Ensure that information is created by the component in a manner that supports downstream information processing and dissemination when possible.

DOJ CIO	Component CIO
7. System interoperability and accessibility. Ensure that information systems built across the enterprise promote interoperability and information accessibility.	7. Ensure that information systems built by the component promote interoperability and information accessibility.
8. Data Life-Cycle Management. Strengthen data life cycle management across the enterprise, including release practices. Incorporate requirements for preservation, records management, accessibility, security, and privacy.	8. Strengthen data life cycle management within the component, including release practices. Incorporate requirements for preservation, records management, accessibility, security, and privacy.
9. Privacy and Confidentiality. Strengthen measures to ensure that privacy and confidentiality are fully protected and that data are properly secured across the enterprise.	9. Strengthen measures to ensure that privacy and confidentiality are fully protected and that data are properly secured by the component.
10. Data Analytics. Enhance the use of enterprise data analytics to advance litigation, investigation, forensics, and business capabilities. Use these tools to detect financial fraud and strengthen security posture.	10. Enhance the use of enterprise data analytics to advance litigation, investigation, forensics, and business capabilities. Use these tools within the component to detect financial fraud and strengthen security posture.
11. Electronic Records. Ensure that electronic records within applications are appropriately retained and disposed of across the enterprise.	11. Ensure that electronic records within applications are appropriately retained and disposed of by the component.
12. Preservation. Preserve Senior Leadership information for eDiscovery requests per DOJ Order 0802 – Management of Preservation Responsibilities.	12. Preserve component information for eDiscovery requests per DOJ Order 0802, Management of Preservation Responsibilities.
13. Burden Reduction. Minimize the paperwork burden on private citizens in support of the Paperwork Reduction Act (PRA). Ensure that information collected from the public, across the enterprise, is limited to the minimum necessary for protection of the public, policy development, effective management, and planning and external reporting. Also, ensure that information is collected by the most efficient, effective, and economical means possible and promote the use of IT for collections.	13. Ensure that information collected from the public by the component is minimal and collected by the most efficient, effective, and economical means possible, and promote the use of IT for the collection. Additionally, ensure that information collections in violation of the PRA are reported to the DOJ Information Manager for immediate resolution, and that all component violations are resolved by the end of the fiscal year.

DOJ CIO	Component CIO
14. Designee. Designate a DOJ IT Information Oversight Manager to act on behalf of the DOJ CIO to oversee enterprise IT information management across the Department, as defined in the Information Technology Information Oversight Policy Statement.	14. Designate a component IT Information Oversight Manager to coordinate with the DOJ IT Information Oversight Manager on behalf of the component CIO to oversee IT information management within the component and act as the component PRA coordinator, as defined in the Information Technology Information Oversight Policy Statement.

J. Information Technology Services Oversight

The DOJ CIO and component CIO must:

DOJ CIO	Component CIO
1. Engineering. Engineer services for multiple solutions through multiple vendors, suppliers, and service providers.	1. Assist the DOJ CIO with engineering enterprise services. Promote the use of these services within the component.
2. Trusted Advisor. Serve as trusted advisor and advocate for the customer. Facilitate transactions, provide professional services, and enable the delivery of efficient and effective enterprise services. Develop tactical and strategic solutions to the problems and needs of customers.	2. Promote enterprise services to component customers.
3. Electronic Marketplace. Create an electronic marketplace that serves as a "one-stop shop" for information and resources regarding DOJ enterprise services. Package services and market to component Services Managers so they stay aware and up-to-date and understand available IT offerings, associated costs, and service level agreements.	3. Promote the use of the DOJ service marketplace among component customers.
4. ITIL Framework. Implement the standard set of practices, known as the Information Technology Infrastructure Library (ITIL) Service Delivery Model, to clearly define the services offered; identify the responsibilities of both customers and service providers; and document reliability, quality, and timelines.	4. Participate in the ITIL service delivery process.

DOJ CIO	Component CIO
5. Service Delivery. Monitor the delivery of enterprise services and collect customer satisfaction measurements. Use measurements to identify services for improvement or retirement.	5. Provide customer feedback on enterprise services.
6. Designee. Designate a DOJ IT Services Oversight Manager to act on behalf of the CIO to oversee enterprise IT services management across the Department.	6. Designate a component IT Services Oversight Manager to coordinate with the DOJ IT Services Oversight Manager on behalf of the component CIO, to oversee enterprise IT services management within the component.

K. Information Technology Customer Relations Oversight

The DOJ CIO and component CIO must:

DOJ CIO	Component CIO
1. Support Service. Establish an enterprise integrated, multi-level support service that is available 24 hours a day, 7 days a week and promotes quick and accurate resolution of both simple and complex requests to enhance productivity.	1. Provide component level support for the service.
2. Customer Life-Cycle Services. Establish consistent enterprise life cycle processes that engage customers from the time they demonstrate interest in the Department's IT services through service termination.	2. Contribute to the development of the service life cycle processes and make use of the service.
3. Designee. Designate a DOJ IT Customer Relations Oversight Manager to act on behalf of the DOJ CIO to oversee enterprise IT strategic management across the Department, as defined in the Information Technology Strategy Oversight Policy Statement.	3. Designate a component IT Customer Relations Oversight Manager to coordinate with the DOJ IT Customer Services Oversight Manager on behalf of the component CIO to oversee enterprise IT customer relations management within the component.

L. Information Technology Security Oversight

The DOJ CIO and component CIO must:

DOJ CIO	Component CIO
1. Designee. Designate a DOJ Chief Information Security Officer (CISO) to serve as: a) the principle security leader for the Department to implement the requirements of FISMA, and b) the DOJ CIO's liaison to federal agencies for all matters relating to enterprise IT security, as referenced in DOJ Order 2640.2F Information Technology Security (or its successor).	1. Work with the CISO to establish and maintain a component-wide IT security program to secure the component's IT systems, networks, and data in accordance with Department policy, procedures, and guidance, as referenced in DOJ Order 2640.2F Information Technology Security (or its successor).

M. Information Technology Accessibility Oversight

The DOJ CIO and component CIO (or component Section 508 Oversight Executive) must implement the Department's Section 508 Program, as defined in DOJ Order 0902 – Accessible Electronics and Information Technology.

Appendix: Information Technology Authorities Matrix

This matrix lists all IT authorities and the policy statements that implement them. Links will be provided when available.

Legislation	SM	VM	AM	WM	EA	IM
Federal Information Technology Reform Act (FITARA) of 2014 ... part of The National Defense Act of 2014, Subtitle D.		X	X	X	X	
Clinger Cohen Act of 1996	X	X	X	X	X	X
Paperwork Reduction Act (PRA)						X
44 U.S.C. Sections 3501-3520						X
Title 5, C.F.R, Part 1320 – Controlling Paperwork Burdens on the Public						X

OMB Guidance	SM	VM	AM	WM	EA	IM
OMB Memorandum M-15-14, Management and Oversight of Federal Information Technology		X	X	X	X	
OMB Circular A-11, Preparation, Submission, and Execution of the Budget		X				
OMB Circular A-130, Management of Federal Information Resources		X	X		X	X
OMB Memorandum M-13-13, Open Data Policy- Managing Information as an Asset						X

Presidential Directive	SM	VM	AM	WM	EA	IM
Revision to the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM)		X				

DOJ Order	SM	VM	AM	WM	EA	IM
DOJ Order 0601 Privacy and Civil Liberties		X				X
DOJ Order 0801 – Records and Information Management						X
DOJ Order 0802 – Management of Preservation Responsibilities						X

Abbreviations:
SM - Strategic Management
VM - Investment Management
AM - Acquisition Management
WM - Workforce Management
EA – Enterprise Architecture
IM – Information Management