ADS Chapter 509

Management and Oversight of Agency Information Technology Resources

Partial Revision Date: 04/12/2021
Responsible Office: M/CIO
File Name: 509_041221

Functional Series 500 – Management Services
ADS 509 – Management and Oversight of Agency Information Technology Resources
POC for ADS 509: Zecharia Kahn, zkahn@usaid.gov

Table of Contents

509.1 OVERVIEW 4

509.2 PRIMARY RESPONSIBILITIES 5

509.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES 10

509.3.1 Key Definitions and IT Covered by this ADS Chapter 10

509.3.2 Strategic Planning 13
509.3.2.1 Agency IT Strategic Plan 13
509.3.2.2 Enterprise Architecture 14
509.3.2.3 Involvement of M/CIO in B/IO/M Strategic Planning 15

509.3.3 Categories of IT Budgetary Resources 16

509.3.4 IT Acquisitions 16
509.3.4.1 IT Acquisition Planning 16
509.3.4.2 Acquisition Review and Approval 19
509.3.4.3 IT Acquisition Post-Approval Requirements 22

509.3.5 Planning for IT Capital Investments 23
509.3.5.1 Guiding Principles for IT Investment Planning 23
509.3.5.2 Stages of Planning for IT Capital Investments 24
509.3.5.3 Changes to the IT Capital Investment Portfolio in the Year of Execution. 25

509.3.6 IT Budget Reporting and Approval 26
509.3.6.1 IT Budget Reporting by B/IO/Ms 26
509.3.6.2 IT Budget Approval and Certification 27
509.3.6.3 IT Budget Submission and Investment Reporting to OMB 28

509.3.7 IT Project Oversight and Management Requirements 29
509.3.7.1 Project Levels 29
509.3.7.2 IT Project Governance 30
509.3.7.3 Additional Federal Requirements for Software Development Projects 31
509.3.7.4 IT Project Performance Reporting and Monitoring 33

509.3.8 IT Portfolio Evaluation and Optimization 34
509.3.8.1 IT Asset and System and Service Inventories 35

509.3.8.2 Review of the Agency's IT Portfolio 36
509.3.8.3 System Decommissioning..... 37

509.3.9 Information Technology Workforce 38

509.4 MANDATORY REFERENCES 39

509.4.1 External Mandatory References 39

509.4.2 Internal Mandatory References 41

509.5 ADDITIONAL HELP 42

509.6 DEFINITIONS 42

ADS 509 – Management and Oversight of Agency Information Technology Resources

509.1 OVERVIEW

Effective Date: 05/20/2019

This Automated Directives System (ADS) chapter defines operational policy for the management and oversight of information-technology (IT) resources at USAID.

This chapter provides general information on the scope of federal laws and regulations relating to IT. Additional guidance is located in the references cited in this chapter including OMB's memorandums, other ADS chapters, and the Standard Operating Procedures (SOPs). Bureaus, Independent Offices, and Missions (B/IO/Ms) are advised to contact the Bureau for Management, Office of the Chief Information Officer (M/CIO) as early as possible when IT resource management issues or questions arise.

This ADS chapter supersedes the following ADS chapters:

- ADS 542: Information Technology Planning, Budgeting, and Investment Control;
- ADS 543: Corporate Information Systems;
- ADS 544: Technical Architecture Design, Development, and Management;
- ADS 546: Acquisition of Federal Information Technology Resources;
- ADS 548: Program-Funded Independent Verification and Validation Reviews; and
- ADS 577: Information Technology Capital Planning and Investment Control

USAID developed this ADS chapter based on the **Federal Information Technology Acquisition Reform Act (FITARA)**, as well as guidance from the Office of Management and Budget (OMB) on how to implement FITARA - **OMB M-15-14: Management and Oversight of Federal Information Technology**.

In addition to FITARA, a number of other laws provide direction for the management and oversight of IT resources across the Federal Government, including, but not limited to, the following:

- **Paperwork Reduction Act**;
- **Chief Financial Officers (CFO) Act of 1990**;
- **Clinger-Cohen Act**;
- **E-Government Act**;
- **Federal Information Security Management Act (FISMA) of 2002**; and
- **Federal Information Security Modernization Act (FISMA) of 2014**.

Those laws, as well as other related regulations and mandates, such as **OMB Circular A-130**, also underpin the policy requirements defined in this ADS chapter.

Information Technology plays an increasingly important role in accomplishing the Agency's mission. USAID strives to manage IT as a strategic asset, to provide cost-effective technology support for accomplishing the Agency's mission.

The requirements defined in this ADS chapter cover various activities in the planning and budgeting for, and the acquisition and execution of, IT resources.

To enhance transparency and accountability, FITARA imposes key requirements on the following roles of Federal departments and agencies:

- Head of Department/Agency;
- Chief Information Officer (CIO);
- Program Leadership;
- Chief Acquisition Officer (Senior Procurement Executive [SPE]);
- Chief Human Capital Officer (CHCO);
- Budget Executives; and
- Chief Financial Officer (CFO).

FITARA requires the Agency CIO to exercise a broad authority to oversee and approve the acquisition and use of IT resources and mandates the CIO to have a significant role in planning, programming, budgeting, and execution decisions that involve IT resources.

509.2 PRIMARY RESPONSIBILITIES

Effective Date: 05/20/2019

a. The **Administrator (A/AID)**, as the head of the Agency, ensures that the Chief Information Officer (CIO) has a significant role in the decision processes for all annual and multi-year planning, programming, budgeting, and execution decisions; related reporting requirements for IT; and the management, governance, and oversight processes related to IT. The Administrator is responsible for fulfilling the duties and requirements outlined in **FITARA**, **OMB Circular A-130**, and other applicable laws, Executive Orders, and policies.

b. In accordance with requirements established in the **Clinger-Cohen Act**, **FITARA**, the **E-Government Act of 2002**, and **OMB Circular A-130**, the **Chief Information Officer (CIO),** reports directly to the Administrator, with daily oversight

provided by the Assistant Administrator for Management (AA/M). The CIO has overall responsibility for the Agency's Information-Resource Management (IRM), as defined in the **E-Government Act of 2002** and **OMB Circular A-130**; and the Agency's IT resources, as defined in **OMB Circular A-130** and **FITARA**; as well as for all functions mandated by the **Clinger-Cohen Act** and **FITARA**. The CIO provides leadership in IT governance and strategic planning, the review and approval of the Agency-wide IT budget, the oversight and approval of IT acquisitions across the Agency, and the management of the Agency IT operations. The CIO, in conjunction with the Agency's budget and procurement executives, is responsible for defining the level of detail used to describe IT resources, distinct from other resources, in the Agency's planning, programming, budgeting, execution, and reporting processes.

c. The **Bureau for Management, Office of the Chief Information Officer (M/CIO)** is responsible for the oversight of the Agency's Information Resource Management, as defined in the **E-Government Act of 2002** and **OMB Circular A-130**; and the Agency's IT resources, as defined in **OMB Circular A-130** and **FITARA**; as well as for all functions mandated by the **Clinger-Cohen Act** and **FITARA**. The CIO, who is the equivalent of a Deputy Assistant Administrator, directly manages M/CIO. The CIO reports directly to the Administrator, as **OMB Circular M-15-14**, the **Clinger-Cohen Act**, and **FITARA** require, with daily oversight provided by the AA/M.

d. **Heads of Bureaus/Independent Offices/Missions (B/IO/Ms)** are responsible for ensuring the following:

- Involving the CIO in the B/IO/M's planning process for the use of IT to achieve the Agency's business and program objectives under USAID's Transformation,
- Obtaining approval from the CIO of the B/IO/M's IT resources,
- Keeping the B/IO/M's IT projects and operations in compliance with the Agency's standards and processes as defined by the CIO, and
- Managing and adequately securing the B/IO/M's information systems.

e. The **Office of the General Counsel (GC)** provides legal counsel and advice on matters related to the statutory and regulatory requirements in the area of managing IT resources.

f. The **Chief Information-Security Officer (CISO)**, in M/CIO, carries out the CIO's information-security responsibilities under the **Federal Information Security Modernization Act (FISMA)** and other related Federal laws, regulations, and policies. The CISO is responsible for integrating information security into the management and oversight of the Agency's IT resources and holding all personnel accountable for complying with the Agency-wide information-security program.

g. The **Senior Agency Official for Privacy (SAOP),** in the Bureau for Management (M Bureau), has overall responsibility and accountability for implementing the Agency's privacy policy and protections, including USAID's compliance with Federal laws, regulations, and policies relating to privacy. The SAOP is accountable for ensuring privacy integration into the management and oversight of the Agency's IT resources.

h. The **Chief Privacy Officer**, in M/CIO, is responsible for managing the Agency's privacy program and implementing the Agency's privacy protections in the planning and execution of the Agency's IT resources.

i. The **Director, Bureau for Management, Office of Acquisition and Assistance (M/OAA)** is responsible for ensuring that the Agency's acquisition policy and practices comply with FITARA requirements and ensuring contract actions that involve IT are consistent with the CIO-approved acquisition strategies and acquisition plans. The Director of M/OAA must also ensure the Agency does not initiate a contract action or interagency agreement that includes covered IT unless the CIO has reviewed and approved it.

j. The **Director, Bureau for Management, Office of Management Policy, Budget, and Performance (M/MPBP)** is responsible for ensuring that B/IO/Ms submit their plans for investing in IT resources from both Program and Operating Expense accounts for the CIO's review. The Director of M/MPBP is also responsible for ensuring that the CIO reviews and approves all portions of the budget request that pertain to IT resources before the Agency submits its annual budget request to the Department of State and OMB.

k. The **Director, Office of Budget and Resource Management (BRM)** is responsible for ensuring B/IO/Ms involve the CIO as early as possible in the budget-planning process that involves IT and for ensuring B/IO/Ms identify program-funded IT in their budget submissions.

l. The **Chief Financial Officer (CFO)**, in the M Bureau, is responsible for:

- Developing and maintaining an integrated Agency financial-management system that complies with applicable accounting principles, standards, and other requirements of Federal financial-management systems;

- Working with the CIO to address and resolve deficiencies related to the Agency's financial-management systems; and

- Accounting for, and reporting on, costs related to the Agency's IT systems, including the capitalization thereof, in conformity with the Statement of Federal Financial Accounting Standards (SSFAS) No. 10, Accounting for Internal Use Software, defined by the Federal Accounting Standards Advisory Board (FASAB).

m. The **Chief Human Capital Officer (CHCO)** is responsible for working with the CIO to develop and maintain an IT workforce that can support the Agency's mission effectively, including by establishing competency requirements for IT staff and defining and implementing strategies for recruiting, training, developing, and retaining IT talent.

n. The **IT Liaison** in each B/IO is responsible for facilitating the planning, budgeting, procurement, and implementation of IT solutions for the B/IO; coordinating IT-related activities with M/CIO to ensure compliance with related Federal laws, regulations, and the Agency's policies; and providing advice to the B/IO leadership on matters related to the use of IT to support the B/IO's operations. The CIO, or their designee, establishes competency standards and serves on the selection panel for all such positions within the Agency.

o. The **Executive Sponsor** is an Agency program or Mission manager who identifies and sponsors potential IT investments based on recognized programmatic or operational needs. An Executive Sponsor is responsible for providing oversight for one or more IT investments throughout their lifecycle.

p. The **Contracting Officer** and **Contracting Officer's Representative (CO/COR)** are responsible for identifying CIO-approved IT in Agency solicitations and contracts, and helping the CIO ensure that IT projects comply with the Agency's standards and processes.

q. The **Planner**, as the designated person responsible for developing and maintaining necessary and written Individual Acquisition Plans (IAPs) (see Federal Acquisition Regulation **(FAR), Subpart 7.101** and **ADS Chapter 300, Agency Acquisition and Assistance Planning**), is responsible for ensuring that B/IOs submit all acquisition strategies and plans that include IT resources to the CIO for review and approval.

r. The **Project Manager (PM)** is responsible for planning, executing, and closing a project related to an IT acquisition. The PM coordinates the project's activities, develops reports for the project, and ensures the project's compliance with the Agency's process guidance for IT projects.

s. The **Management Operations Council (MOC)**, as the Agency's executive governance board for directing management reforms and improvement initiatives, is responsible for overseeing the re-engineering of business processes and major Agency IT initiatives. The MOC is responsible for reviewing the Agency's IT capital-investment proposals and for making recommendations to the Administrator based on the Administrator's management priorities and the USAID Transformation.

t. The **IT Steering Subcommittee (ITSS)** of the MOC, sponsored by the CIO, is responsible for providing executive guidance to the management and oversight of the Agency's IT resources, including providing input to the development of the Agency's IT

strategies, evaluating and prioritizing the Agency's IT capital investments, and exercising executive oversight for the Agency's major IT programs.

u. The **Investment Review Committee (IRC)**, in M/CIO, is responsible for providing preliminary recommendations to the CIO and the ITSS regarding which projects to fund based on the Agency's priorities, available resources, and strategies defined in the **USAID IT Strategic Plan (ITSP)** and by the needs of USAID's Transformation. The IRC is also responsible for the ongoing monitoring and evaluation of IT projects and investments.

v. The **Agency IT Roundtable** is an IT planning-advisory group sponsored by the CIO that consists of IT Liaisons from B/IOs. The Agency IT Roundtable is responsible for providing input to the Agency's IT strategic planning; assessing the IT needs of B/IOs and the entire Agency; and providing input on future IT investments to the CIO, ITSS, and MOC.

w. The **Bureau for Management, Office of the Chief Information Officer, Planning and Administration Division (M/CIO/PAD)** is responsible for providing oversight and reporting for the Agency's IT budgetary resources, managing performance-tracking and reporting of IT programs and projects, and coordinating planning activities for IT capital investments.

x. The **Bureau for Management, Office of the Chief Information Officer, Information and Process-Management Division (M/CIO/IPM)** is responsible for:

- Developing and updating the Agency's ITSP,
- Establishing and maintaining the Agency's Enterprise Architecture,
- Establishing and managing the Agency's technology standards and IT governance and processes,
- Developing and maintaining the Agency's policy for managing information resources, and
- Conducting periodic audits and program reviews of the Agency's IT projects.

y. The **Bureau for Management, Office of the Chief Information Officer, IT Service-Delivery Division (M/CIO/ITSD)** is responsible for serving as the point of contact for B/IO/Ms to submit their IT needs and acquisition requests; assessing IT acquisition requests submitted by USAID B/IO/Ms for routing to the appropriate decision-making process; and providing execution oversight for IT projects with significant cost, complexity, or impact on USAID's mission or workforce.

z. The **Bureau for Management, Office of the Chief Information Officer, Information Assurance Division (M/CIO/IA)** is responsible for ensuring USAID's IT

investments, regardless of funding source, comply with all information-security and privacy requirements under Federal laws, regulations, and mandates.

aa. The **Bureau for Management, Office of the Chief Information Officer, IT Operations Division (M/CIO/ITO)** is responsible for developing, implementing, operating, and enhancing enterprise business applications and the Agency's technology infrastructure. In addition, M/CIO/ITO is responsible for establishing and maintaining the Agency's inventories of enterprise IT assets, systems, and services.

509.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 05/20/2019

This section defines policy directives and required procedures for various activities in the management and oversight of IT resources at USAID, including key definitions and the scope of IT covered by this ADS chapter; strategic planning; planning for IT capital investments; reporting on, and approval of, the Agency's IT budget; the acquisition of IT resources; the execution of IT projects; and the evaluation and optimization of the Agency's IT portfolio.

509.3.1 Key Definitions and IT Covered by this ADS Chapter

Effective Date: 05/20/2019

OMB M-15-14: Management and Oversight of Federal Information Technology defines "IT resources" as:

a. Agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of information technology;

b. Acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but

c. Does not include grants to third parties that establish or support information technology not operated directly by the Federal Government.

OMB M-15-14: Management and Oversight of Federal Information Technology defines "Information technology" as:

a. Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are 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; where

b. Such services or equipment are “used by an Agency” if used by the Agency directly or if used by a contractor under a contract with the Agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

c. The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.

d. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

IT to which this ADS chapter does NOT normally apply is the following:

- **IT procured for public-sector entities in host countries:** This ADS chapter does not apply to IT procured under an award to be provided directly and immediately to a host country, because IT procured for host-country governments does not meet the definition of “used by the Agency.” Examples of IT procured for host countries include a health-information management system purchased for a host-country government or personal computers procured for public schools in a host country.

  However, if the Agency or Agency contractor first procures and uses IT and then transfers it to a host country, the IT is considered to be “used by the Agency.” In this circumstance, the IT would be subject to the policy in this and other ADS chapters for the time period before the Agency or an Agency contractor transfers it to the host country. For example, in a contract that requires a USAID contractor to use a health-survey tool, if the contractor uses the tool for two years in the performance of the contract, and then transfers the tool to the host-country government, then it is considered to be IT as defined in this ADS chapter until the Agency or an Agency contractor transfers it to the host country.

- **IT procured under grants and cooperative agreements:** This ADS chapter does not normally apply to IT procured under grants or cooperative agreements (including grants under contracts), because it is inappropriate to procure IT for the Agency’s use under assistance awards. The distinction between grants/cooperative agreements and contracts is more fully described in **ADS 304, Selecting the Appropriate Acquisition and Assistance (A&A) Instrument**. In summary, under the **Federal Grant and Cooperative Agreement Act**, grants and cooperative agreements transfer anything of value to a recipient to carry out

a public purpose, unlike contracts, which the Federal Government uses for its direct benefit or use. The Agency must not procure IT for its own use through an assistance award.

- **Incidental IT:** This ADS chapter does not apply to IT acquired by a contractor incidental to a contract that does not require the use of equipment or a system. Examples of incidental IT include a contractor's corporate human-resources system, financial-management system, or email system, as the contractor acquired them solely to assist in managing its own corporate resources assigned to a U.S. Government contract. Another example of incidental IT is a project-management tool procured by a contractor to manage a hospital-construction project in a host country.

IT procured for host countries, awarded under grants or cooperative agreements, and incidental IT, are not normally within the scope of FITARA. In the unusual circumstance that the Agency could use the IT in these categories, the B/IO/M must consult with the M/CIO prior to the procurement of the IT.

The criteria and examples listed above for assessing the scope of FITARA provide guidance on how the OMB definitions apply to USAID. They do not cover every circumstance, and B/IO/Ms must consult with M/CIO in situations in which the application of FITARA is unclear. IT that is not specifically excluded should be considered to be within the scope of this ADS chapter until an M/CIO review has excluded it. USAID has identified criteria that can affect whether IT is "used by the Agency." The CIO will consider these criteria when determining whether IT falls outside the scope of FITARA:

a. Whether the Agency owns the IT;

b. How Agency personnel use the IT;

c. Whether the IT collects, maintains, or processes Federal information;

d. The Agency's rights to, and restrictions with, the data;

e. Whether the IT is interconnected to an Agency system;

f. The purpose of the contract under which the IT is being procured; and

g. The role the IT plays in the delivery of a product and/or services under the contract.

IT to which this ADS chapter applies:

This ADS chapter applies to IT "used by the Agency." Whether the Agency procures IT or an awardee acquires it, it is covered by this, and other ADS chapters, as long as it meets the criteria for "used by the Agency," as defined by OMB. This could mean such services or equipment used by the Agency directly; or used by a third party under a contract with the Agency that requires either the use of the services or equipment, or requires the use of the services or equipment to a significant extent in the performance of a service, or the furnishing of a product.

To consult with M/CIO on the application of this policy, FITARA, and other applicable regulations, email: **ITAuthorization@usaid.gov**.

509.3.2 Strategic Planning

Effective Date: 05/20/2019

Information Technology is a key enabler for USAID's mission, interwoven into all aspects of the Agency's operations, while helping the Agency adapt to ever-changing challenges and opportunities. For the Agency to leverage IT effectively, the CIO will conduct strategic planning with key stakeholders from B/IO/Ms to develop and maintain an Agency **ITSP**. In addition, B/IO/Ms must view IT as a strategic tool and engage the CIO in strategic and program planning processes to explore the best ways to leverage IT to achieve development objectives.

509.3.2.1 Agency IT Strategic Plan

Effective Date: 05/20/2019

In compliance with **OMB Circular No. A-130**, the CIO must develop and publish an Agency Information Resource Management (IRM) Strategic Plan, sometimes referred to as the IT Strategic Plan (ITSP) (referred to as ITSP hereafter in this ADS chapter). The Agency ITSP, as also required by **OMB Circular No. A-11**, provides a description of how various IT-management activities help accomplish the Agency's mission and ensure the integration of decisions on IT resources with Agency-wide planning, budget, procurement, financial management, human-resources management, and program decisions.

The Agency ITSP must define the goals and objectives for the management of information resources for the next three to five years and document the strategies designed to achieve the defined goals and objectives. The ITSP must also establish performance measurements for the defined objectives, including performance measures on how IT investments support the Agency's programs. The CIO must produce a report on the progress of achieving the goals on an annual basis. The CIO must also report annually, to the Administrator, the effectiveness of the Agency information-security program.

The CIO must update the ITSP annually to address changing priorities and evolving strategies.

As part of IT strategic planning, the CIO must benchmark Agency IT-management processes against appropriate public- and private-sector organizations and/or processes. In addition, the CIO must ensure that Agency processes and policies are analyzed and revised as appropriate before making major IT investments.

As required by OMB Circular No. A-130, the Agency ITSP must also support the goals of the Agency Strategic Plan required by the **Government Performance and Results Modernization Act of 2010 (GPRA Modernization Act)**.

M/CIO/IPM is responsible for managing the development and update of the Agency ITSP and must engage IT Liaisons as well as business and program executives from B/IO/Ms in the development and update process.

The Agency ITSP serves as the cornerstone for IT capital-investment planning activities, including overarching and high-level strategic initiatives. The ITSP guides the selection of Agency IT capital investments. B/IO/M IT capital investments must align with the ITSP. M/CIO must regularly review the ITSP to ensure USAID's IT infrastructure and IT offerings enable the Agency to meet its evolving business needs.

509.3.2.2 Enterprise Architecture

Effective Date: 04/12/2021

Enterprise Architecture (EA) is a framework for analyzing organizational business needs, depicting the relationships between business functions and IT components, and defining the roadmap for the enterprise transition from the current to the target state by leveraging IT.

As required by the **Clinger-Cohen Act** and **OMB Circular No. A-130**, M/CIO must develop the Agency enterprise architecture to guide the planning, design, implementation, and sustainment of IT solutions. The Agency's EA must:

- Align to the Agency ITSP;
- Include business, technical, data, and security components;
- Incorporate Agency plans for significant upgrades, replacements, and disposition of information systems when the systems can no longer effectively support program or business functions; and
- Provide information about the Agency IT portfolio and associated costs at all stages of the lifecycle for IT services, systems, applications, and tools deployed in the organization at any given point of time.

A key component of the USAID EA is the **Enterprise Transition Roadmap (ETR)**. An ETR must include:

- Current and future architecture states,
- A transition plan to achieve the future state, and
- Supporting artifacts representing both the current and future state.

The USAID ETR creates awareness, transparency, and visibility within the Agency, facilitates cross-organization planning, and ties projects and budgets to strategy. The ETR creates a direct *line-of-sight* from projects to the strategy they support and provides authoritative information for planning, decision making, and management.

M/CIO/IPM is responsible for developing and maintaining the Agency EA.

Each B/IO/M must ensure the IT capital investments made by the B/IO/M are aligned with the Agency EA (see section **509.3.4** and **ADS 549.3.5.9** for additional guidance).

509.3.2.3 Involvement of M/CIO in B/IO/M Strategic Planning

Effective Date: 05/20/2019

In addition to providing essential support to USAID's core back-office operations, such as managing human capital and finances, IT is critical to strategic planning and the execution of international development and humanitarian-assistance programs.

USAID B/IO/Ms must engage IT Liaisons for the B/IOs and M/CIO in the strategic-planning process related to IT capital investment and must seek input and advice from the M/CIO to:

- Explore the best approaches for leveraging technologies in international development and humanitarian programs and enhancing evidence-based decisions;
- Minimize duplication across the Agency of IT investments required to support program-related activities, such as monitoring, evaluation, and collaborative learning and adapting; and
- Ensure decision-makers at the Agency clearly understand the business needs for IT solutions and take an enterprise approach to drive effective and cost-efficient IT resource use.

USAID overseas Missions should consult with M/CIO by contacting **clientservices@usaid.gov** as they develop their Country Development and Collaboration Strategies (including Regional Development and Collaboration Strategies) with regard to an information-technology strategy and solutions required to support development and humanitarian objectives, as well as to execute the plans for monitoring, evaluation, and collaborative learning and adapting.

B/IOs with large IT spending (*e.g.*, $5 million or more annually), including Program-funded IT resources, must develop an IT strategic plan (ITSP). B/IOs must engage M/CIO in the IT strategic-planning process and ensure their ITSP aligns with the Agency's ITSP.

509.3.3 Categories of IT Budgetary Resources
Effective Date: 05/20/2019

Four types of IT budgetary resources support USAID's operations:

1. **Central IT Operating Expense (OE):** Central budgetary resources that fund the ongoing operations and maintenance of the Agency's IT infrastructure, enterprise business systems, and services, including, but not limited to, the Agency's networks, data centers, service-desk support, and corporate/enterprise information systems. This category includes the USAID IT Cost Center budget, cost-recovery funds received by M/CIO from B/IO/Ms for providing services and support to program-funded staff, and chargeback to B/IO/Ms for special support provided by M/CIO.

2. **Agency IT Capital Investment Fund (CIF):** Central budgetary resources used for upgrades to IT infrastructure and the development, modernization, and enhancement (DME) of key Agency information systems.

3. **Program-Funded IT:** Budgetary resources from program budgets used to pay for IT equipment, systems, and services.

4. **OE-Funded IT by B/IO/Ms:** Budgetary resources from B/IO/Ms' OE funds for IT equipment, systems, and services in support of operations of B/IO/Ms.

509.3.4 IT Acquisitions
Effective Date: 05/20/2019

Under FITARA, the CIO must review and approve all IT acquisitions. B/IO/Ms must identify planned IT investments as early as possible, and engage M/CIO in the planning and execution of the IT investments.

This subsection provides policy and procedures for CIO's oversight of IT acquisitions. All acquisitions that contain an IT component must be approved by CIO at the earliest stage in which IT is identified.

509.3.4.1 IT Acquisition Planning
Effective Date: 04/12/2021

All Agency IT acquisitions, including the acquisition of services that contain an IT component, must also follow the policy and procedures prescribed in the ADS 300 Series and the Agency's **IT Purchase Guidance**. This additional guidance describes

M/CIO-approved product lists and/or dollar thresholds that satisfy the requirement for CIO approval.

a. Considerations in IT Acquisition Planning

When planning for procuring an IT solution to address a business need, the Planner must consult with the IT Liaison designated for their B/IO to identify whether a solution already exists within the Agency that satisfies the business need.

When conducting an IT acquisition, all B/IO/Ms must adhere to:

- Agency policies, including **ADS 300**, **ADS 302**, **Acquisition and Assistance Policy Directive (AAPD) 16-02 (Revised)**, and **ADS 549.3.5.9**.

- Relevant federal mandates, such as **41 U.S.C. 2308, Modular Contracting for Information Technology**, and **44 U.S.C. Chapter 35, Subchapter II, Information Security**.

- OMB policy, including but not limited to, **OMB Circular A-130, Managing Information as a Strategic Resource**, and the Category Management Policies for improving the acquisition and management of common IT, such as:

    - Laptops and Desktops (**M-16-02**),
    - Software Licensing **(M-16-12**)
    - Mobile Devices and Services (**M-16-20**), and
    - Completing the Transition to Internet Protocol Version 6 (IPv6) (**M-21-07**).

- FAR, including the planning requirements in **FAR Subpart 7.1, Acquisition Plans**, and **Part 10, Market Research**.

In addition, a B/IO/M planning an IT acquisition that is not pre-approved by the CIO under the **IT Purchase Guidance** must:

- Develop a comprehensive Cost-Benefit Analysis of all procurement requirements based upon market research, which includes an analysis of alternatives (including existing Agency IT resources/solutions).

- Consider and apply cloud computing solutions if a secure, reliable, cost-effective cloud-computing option exists, to maximize capacity use, improve IT flexibility and responsiveness, and minimize costs. Existing Agency cloud environments should be utilized.

- Make use of adequate competition, analyze risks (including supply-chain risks) associated with potential contractors and the products and services they provide, and allocate risk responsibility between the government and the contractor when acquiring IT.

- Conduct definitive technical, cost, and risk analyses of alternative design implementations, including consideration of the full lifecycle costs of IT products and services, including but not limited to, planning, analysis, design, implementation, sustainment, maintenance, re-competition, and retraining costs, scaled to the size and complexity of individual requirements.

- Consider existing federal solutions or shared services when developing planned information systems, available within the same agency, from other agencies, or from the private sector to meet Agency needs to avoid duplicative IT investments.

- Ensure that decisions to improve existing information systems with custom-developed solutions or the development of new information systems are initiated only when no existing alternative private-sector or governmental source can efficiently meet the need, taking into account long-term sustainment and maintenance.

- Structure acquisitions for major IT investments into useful segments, with a narrow scope and brief duration, to reduce risk, promote flexibility and interoperability, increase accountability, and better match mission need with current technology and market conditions.

- For all IT software development projects, appropriately implement incremental development and modular approaches as defined in the **OMB Contracting Guidance to Support Modular Development,** issued June 14, 2012.

- Institute performance measures and management processes to monitor and compare actual performance against planned results.

- Promote innovation in IT acquisitions, including conducting market research in order to maximize use of innovative ideas.

- Include security, privacy, accessibility (Section 508 compliance), records management, and other relevant requirements in solicitations (see **509.4.2**).

- Consistent with the FAR, contracts for custom software development must include provisions that address government data rights and deliverable requirements (see **ADS 547maa** for more detailed requirements related to the custom software development, and see ADS 318 for guidance on intellectual property rights and issues related to software products developed).

b. Identification of IT in A&A Plan System and GLAAS

To facilitate the identification of IT components in Agency acquisitions, Planners, requestors, CORs, and COs must indicate in both the A&A Plan System and the

Agency's Global Acquisition & Assistance System (GLAAS) whether planned actions, requisitions, solicitations, or awards include IT. Planners/CORs must follow Agency policy for submitting planned IT acquisitions to the M/CIO and receiving CIO approval for all IT acquisition strategies and plans, prior to the actual acquisition.

Upon request by M/CIO, B/IO/Ms planning/conducting acquisitions that contain IT must provide any additional information required in support of the CIO's management and oversight of IT acquisitions.

509.3.4.2 Acquisition Review and Approval

Effective Date: 05/20/2019

The CIO must review and approve all acquisitions or interagency agreements (such as those used to support purchases through another Department or Agency) that include IT (see **ADS 300**) at the strategy, plan, or requirement (as described in **FAR Part 7**) level. The request for approval must be submitted to **ITAuthorization@usaid.gov**.

When submitting an IT acquisition request for the CIO's approval, the Planner must provide sufficient information to support the review by the CIO, including:

- An Individual Acquisition Plan (IAP) if one is created (see **ADS 300** for detailed information about IAPs); or
- A Statement of Work (SOW) and Independent Government Cost Estimates (IGCE).

The CIO, or their designee, may request additional information, such as detailed market research and alternative analysis, deemed necessary to support the review.

In support of the CIO's role in reviewing and approving IT acquisitions, the Director of M/OAA must work closely with the CIO to develop and implement an Agency-wide process to ensure all acquisitions that include significant IT are:

- Led by personnel with appropriate Federal acquisition certifications (FACs), including specialized IT certifications, as appropriate;
- Reviewed for opportunities to leverage acquisition initiatives, such as shared services, category management, strategic sourcing, and incremental or modular contracting, and use such approaches as appropriate;
- Supported by cost estimates (IGCE) reviewed by the CIO;
- Adequately implement incremental development; and
- Reviewed and approved by the CIO.

a. <u>Acquisition Review Criteria</u>

When evaluating IT acquisition requests, M/CIO must consider the following factors:

- Alignment with the Agency's mission and program objectives, including the Transformation, in coordination with program leadership;
- Alignment with the Agency's ITSP and Enterprise Architecture, including the ETR;
- Consistency with **Agency IT standards** and mandatory contract vehicles;
- Promotion of innovative solutions;
- Leverage of acquisition initiatives such as shared services and category-management;
- Appropriateness of contract type for IT-related resources, including the application of modular contracting principles and strategic sourcing;
- Accuracy of need description in SOW related to IT to be acquired;
- Ability to deliver functionality in short increments;
- Inclusion of government-wide IT requirements, such as accessibility, information security, and privacy safeguards;
- Accuracy of cost estimates;
- Availability of sufficient funding to support system lifecycle-management needs;
- Opportunities to migrate from end-of-life software and systems, and to retire those systems; and
- Technology considerations such as interoperability, scalability, and sustainability of the proposed solution.

b. Acquisition Review Process

The acquisition review conducted by M/CIO depends on the type of IT products and services to be procured. The common type of IT products and services include the following:

- Cloud/Web Hosting Services including free services;
- System/application development including enhancement to an existing system/application;

- Procurement of a shared service from another Federal agency such as HRConnect from the Department of Treasury;
- Commercial off-the-shelf (COTS) software products or licenses, including no-cost software;
- Software components (plug-ins, add-ons, extensions) regardless of cost;
- Website subscriptions, including free subscriptions;
- Laptops, desktops, and associated accessories such as mouse, keyboards, *etc.*;
- Multi-functional devices (MFDs) or network printers;
- Tablets and smartphones;
- Computer servers and other hardware;
- Network equipment such as switches, routers, *etc.*;
- Office equipment such as desk phones; and
- IT service personnel such as personal service contractors who work on development of IT solutions and/or support IT operations.

B/IO/Ms must use the **IT Purchase Guidance** to determine the review and approval process required. This additional guidance describes M/CIO-approved product lists and/or dollar thresholds that satisfy the requirement for CIO approval.

When planning system/application development, including enhancement to an existing system, a B/IO/M must provide sufficient information in support of the review by M/CIO. The minimum information required is as follows:

- A clear problem statement;
- An estimate of a five-year lifecycle cost, including DME and related O&M;
- An analysis of alternative approaches/solutions;
- Business benefits of the system/application to be developed/enhanced including estimated ROI;
- An estimated acquisition timeline; and

- Whether the proposed acquisition was part of an IT capital investment approved by the ITSS (see **509.3.4.3** for information on the future year IT capital investment process).

When reviewing an IT acquisition request, M/CIO compares the request against the previously approved IT budget for the B/IO/M planning the acquisition (see **509.3.6**). If the IT acquisition being planned was not in the approved IT budget, the requestor may be required to provide a justification for the deviation.

After receiving the required information from the requesting B/IO/M, the CIO must decide within 15 business days to:

- Approve the planned acquisition without condition,
- Approve the planned acquisition with condition, or
- Reject the planned acquisition with an explanation.

For a contract or agreement for a non-major IT investment, as defined in the annual information technology capital planning guidance from OMB, the CIO may delegate approval of the contract or agreement to an individual who reports directly to the CIO.

509.3.4.3 IT Acquisition Post-Approval Requirements

Effective Date: 05/20/2019

After the CIO approves an IT acquisition request, including an acquisition or modification that contains an IT component or service, or an IAP that includes IT, the B/IO/M can proceed to procure the IT resources planned for the acquisition.

The COR for the acquisition must notify M/CIO (**ITAuthorization@usaid.gov**) when the IT procurement is completed, *i.e.*, a contract is awarded or IT equipment is purchased, or subscription to an online service is made, *etc*.

B/IO/Ms must also notify M/CIO if a significant change to the planned acquisition occurs. For example, if a B/IO/M decides to cancel the planned IT acquisition, the B/IO/M must notify M/CIO about the change. If a B/IO/M makes a change to a planned IT acquisition previously approved by the CIO, *e.g.*, the dollar amount for the planned acquisition is significantly changed, the B/IO/M must notify M/CIO, and additional review and approval by the CIO may be required.

M/CIO must update the USAID IT asset and/or system inventory after an IT procurement is completed. In compliance with **Public Law No: 114-210 (MEGABYTE Act of 2016)** and **OMB M-16-12**, M/CIO must track software licenses purchased by USAID. Specific requirements and procedures for IT asset management, including software license management, are defined in **ADS 547, Property Management of IT Resources** and **ADS 547maa, Limits on Custom Developed Software**.

509.3.5 Planning for IT Capital Investments
Effective Date: 05/20/2019

Planning for IT capital investments refers to activities conducted to make decisions on future IT capital investments. Such investments make improvements in the Agency's IT infrastructure, information systems, and services; they do not include the financial resources allocated to support ongoing operations and maintenance (O&M) of the existing IT infrastructure, information systems, and services. The Agency has instituted a planning and review process for capital investments that imposes additional requirements on the procurement of IT that meets certain criteria (see section **509.3.5.2** for more information on the investment review process).

The following three criteria describe when a B/IO/M must go through the planning and review process for IT capital investments:

1. The Agency's IT CIF funds the investment; OR

2. Program-funds are paying for the investment, which involves the development, enhancement, or modernization of an IT solution, AND the investment has an estimated five-year lifecycle cost that exceeds $5 million; OR

3. Program funds are paying for the investment, which involves the development, enhancement, or modernization of a mission-critical system – see section **509.6** for the definition of a "mission-critical system."

If a B/IO/M is considering an IT solution that falls under any of these three scenarios, it must complete the investment planning and review process before undergoing the acquisition process.

IT solutions that do not meet any of the three scenarios above may still require CIO review and approval per the requirements defined in this ADS chapter.

509.3.5.1 Guiding Principles for IT Investment Planning
Effective Date: 05/20/2019

The following principles guide the Agency's review of proposed IT capital investments:

- **Support for the Agency's Transformation** - IT capital investments that support the accomplishment of the Agency's Transformation, as well as the Agency's management priorities as defined by the Management Operations Council (MOC).

- **Strategic Alignment** - IT capital investments that align with the **Department of State and USAID Joint Strategic Plan** (JSP); the **USAID ITSP**; and Federal government-wide strategies, such as Federal Shared Service Initiatives, Cloud First Policy, *etc*.

- **Return-on-investment (ROI)** - Proposed IT capital investments need to demonstrate a positive projected ROI measured against the ROI of other potential IT investments that are competing for limited resources. The ROI calculation could include improved performance against the JSP, as well as for programs and projects. The ROI could also include reduced costs, improved quality or accuracy, increased speed, enhanced flexibility, and increased satisfaction of customers or employees.

- **Portfolio Focus** – B/IOs must plan IT capital investments in relation to all current and proposed investments in IT across the Agency to minimize duplicate spending and maximize reuse.

- **Architecture-Driven** - IT capital investments must align with the USAID Enterprise Architecture and be consistent with the USAID ETR.

- **Executive Involvement** - The CIO must review and approve the Agency's IT capital-investment portfolio. Through the USAID MOC, including the IT Steering Subcommittee (ITSS), USAID senior executives from B/IOs must be involved in selecting, monitoring, and evaluating IT investments.

509.3.5.2 Stages of Planning for IT Capital Investments

Effective Date: 05/20/2019

The IT capital investment planning process at USAID includes two phases: Pre-Select and Select.

Pre-Select: Includes the identification of one or more business problems, an evaluation of alternative solutions (including existing Agency IT solutions), recommendation of one or more IT capital investments as the solution(s), and the selection of an Executive Sponsor and point of contact to support the investment submission and review process. During this initial stage:

- The B/IO prepares a Project Operation Description Document (PODD) to depict the business case for each proposed IT capital investment,

- The M/CIO IRC conducts a preliminary review and analysis, and

- The IRC then presents its recommendations to the CIO.

Select: Includes the CIO's initial review of proposed IT capital investments in consideration of Agency priorities, resource-constraints, and alignment with the Agency's ITSP. During this stage, the CIO will:

- Examine additional details for the IT capital investments identified in the Pre-Select phase;

- Confirm the applicable level of detail required for further consideration;

- Provide the preliminary ranking of the proposed IT capital investment to the Executive Sponsors; and

- Schedules the evaluation and prioritization of the proposed IT capital investments by the ITSS and the MOC, where appropriate.

After the recommendations of the ITSS and MOC, the Administrator/Deputy Administrator makes the final decision to approve (select) or reject the proposed IT capital investment(s). The CIO will notify Executive Sponsors of the decisions by the Administrator/Deputy Administrator.

If a proposed IT capital investment is not selected, the Executive Sponsor may re-submit it to the ITSS for consideration in the following year.

More detailed information about Pre-Select and "Select" process can be found in the **Guide for the USAID IT Capital Investment Planning Process**.

509.3.5.3 Changes to the IT Capital Investment Portfolio in the Year of Execution

Effective Date: 05/20/2019

As depicted in **509.3.4.3**, IT capital investment decisions are made through the Pre-select and Select process usually more than a year before the funding becomes available for execution. A number of changes could occur before the selected investments are actually implemented, for example:

- Budgetary resources for IT capital investments are less than expected, *e.g.*, the CIF budget might be reduced significantly in the approved Agency budget;

- A new mandate from the Congress or the White House is issued and implementation of the mandate requires the allocation of IT capital investment funds, *e.g.*, a cybersecurity initiative from the White House might require a new investment in a network attack detection and prevention tool; or

- A new priority is created by the Administrator and a new IT capital investment is needed to support the new priority, *e.g.*, an initiative to improve Agency-wide communication and collaboration with implementing partners might require a new capital IT investment to improve technology capabilities in support of collaboration with external communities.

To address an increase/decrease in funding for IT capital investments or changes in investment priorities, M/CIO/PAD must evaluate, in the beginning of each fiscal year or right after the current year Agency budget is approved by Congress and the President, approved budgetary resources for IT capital investments and assess other changes that may affect the IT capital investment allocation for the current fiscal year. After

consulting with key stakeholders, such as Executive Sponsors for IT capital investments approved in the previous year, M/CIO/PAD must then propose any necessary adjustments to the IT capital investment portfolio for the current year.

After the CIO's review and preliminary approval of the revised IT capital investment portfolio, M/CIO/PAD must present the revised portfolio to the ITSS. The ITSS is then responsible for evaluating the proposed adjustments and making decisions on whether the revised IT capital investment portfolio should be approved or any additional changes need to be made.

Once the future year IT capital investments are selected through the process described in **509.3.5**, those selected investments must be reported in IT budget submissions, together with other planned IT spending.

509.3.6 IT Budget Reporting and Approval

Effective Date: 05/20/2019

Under the **Clinger-Cohen Act** and **FITARA**, the CIO maintains overall authority for the approval and oversight of USAID's Agency-wide IT budget. The CIO's oversight of the Agency-wide IT budget is critical to accomplish the following:

- Enhance IT budget transparency,
- Improve cost-effectiveness of IT capital investments,
- Minimize potentially duplicate IT capital investments, and
- Implement information security and privacy safeguards.

This section defines the requirements for Agency-wide IT budget reporting, review, and approval.

509.3.6.1 IT Budget Reporting by B/IO/Ms

Effective Date: 05/20/2019

To ensure visibility of the Agency's IT budget and support the CIO's oversight, each B/IO/M must report planned IT spending in an annual budget submission to M/CIO.

The IT budget reporting by each B/IO/M must include the following:

- Proposed IT spending from an OE account;
- Proposed IT spending from program funds used to support Agency or program operations; and
- Proposed IT spending from a Trust Fund account, if any.

The Director of M/MPBP must work with the CIO each year to develop or update specific guidance and instructions for the submission of B/IO/Ms' IT budgets, however funded. This IT budget information is collected as part of the B/IO/Ms' annual OE budget submission. When preparing the IT budget reporting guidance and instructions, the Director of M/MPBP and the CIO must incorporate OMB's requirements with regard to Technology Business Management (TBM) an IT management framework that implements a standard IT spend taxonomy.

B/IO/Ms must follow the guidance and instructions issued by M/MPBP when reporting the IT budget.

The Director of BRM, when issuing annual guidance for Bureau Resource Requests (BRRs), must direct B/IOs to report IT spending to be funded by program budget to M/CIO and follow the specific instructions from M/MPBP.

509.3.6.2 IT Budget Approval and Certification

Effective Date: 05/20/2019

As required by FITARA, the CIO must review and approve the Agency-wide IT budget request. The CIO must also certify her/his approval in the Agency's budget submission to OMB.

a. <u>CIO Approval and Certification of Agency Budget Submission</u>

After reviewing the IT budget submissions by all B/IO/Ms, the CIO must determine whether she/he approves the Agency's proposed IT budget. In addition, USAID budget justification materials in the initial submission to OMB must include a statement that affirms:

- The CIO has reviewed and approves the major IT investments included in this budget request;
- The Director of M/MPBP, the Director of BRM, and the CIO jointly affirm that the CIO had a significant role in reviewing planned IT support for major program objectives and significant increases and decreases in IT resources; and
- The IT Portfolio includes appropriate estimates of all IT resources included in the budget request.

The Director of M/MPBP and the Director of BRM must obtain the CIO's approval for the Agency-wide IT budget request contained in the annual Agency IT budget, before the Agency submits its budget request to the Office of U.S. Foreign Assistance Resources (F Bureau) for combined submission to OMB, or consistent with OMB budget guidance.

b. <u>CIO Approval of Reprogramming of Funds for IT Resources</u>

In addition to the requirement for the CIO's approval and certification of the Agency's budget submission to OMB, the CIO must approve, under FITARA, any movement of funds for IT resources that requires Congressional notification. For example, if the Agency proposes to reallocate a portion of the IT Capital Investment Fund to the USAID Overseas Physical Security Improvement Program, the CIO must approve such reallocation before the Bureau for Legislative and Public Affairs (LPA) submits the Congressional Notification for reprogramming.

The Director of M/MPBP and the Director of BRM must obtain the CIO's approval for the movement of funds for IT resources before LPA submits the Congressional Notification for reprogramming.

As required by FITARA, the CIO may not delegate the authority to review and approve the reprogramming of any funds made available for IT programs.

509.3.6.3 IT Budget Submission and Investment Reporting to OMB

Effective Date: 05/20/2019

While USAID's overall budget at a high level is included in the combined Department of State, Foreign Operations, and Related Programs Budget submission, the Agency submits a detailed USAID IT budget separately to OMB. In addition, all updates to USAID's IT capital investments must be reported to OMB for publishing on the **Federal IT Dashboard (ITDB)** on a regular basis.

The annual IT budget submission must follow OMB's Capital Planning and Investment Control (CPIC) guidance and any published updates to **OMB Circular No. A-11**.

The annual submission of the Agency IT budget must include all funding needs associated with all four categories of IT resources described in **509.3.3** of this ADS chapter. M/MPBP is responsible for collecting IT budget information, regardless of source of funding, from all B/IO/Ms. M/CIO/PAD is responsible for reviewing IT budget submissions by the Operating Units (OUs) and submitting the Agency IT budget information to OMB.

Managed by OMB, the **Federal ITDB** was created to provide the public with the ability to view details of Federal IT investments online and to track their progress over time. USAID is required to provide IT budget information to OMB for publication to the Federal ITDB.

The approximate timeline for the annual IT budget reporting to OMB is usually as follows:

- August–September FYXX - Agency-approved budget year request is submitted to the Federal ITDB; and

- January–February FYXX - Submission of IT Passback version of the budget year request to the Federal ITDB.

M/CIO/PAD is responsible for reviewing the submissions by B/IO/Ms and is responsible for submitting the approved version to OMB. B/IO/Ms are responsible for providing M/CIO/PAD with documentation to support the reporting requirements upon request. Subsequent updates to the USAID budget are submitted to the Federal ITDB.

In addition to the annual IT budget submission, M/CIO/PAD is responsible for coordinating and submitting periodic IT capital investment performance updates to the Agency's submission as specified in OMB's specific guidance, which is updated and published annually. B/IO/Ms must support M/CIO/PAD in collecting required information for IT capital investments funded by the OUs.

509.3.7 IT Project Oversight and Management Requirements

Effective Date: 05/20/2019

An IT project is a set of activities conducted to implement an IT service or solution over a defined amount of time and with an allocated budget, for the purpose of delivering value to the Agency.

To ensure the successful implementation of USAID IT projects, the CIO must provide oversight and define the Agency guidance for the System Development Lifecycle (SDLC) process, including required project artifacts. All USAID IT projects must be executed in compliance with the **USAID IT Project Management Guide**.

509.3.7.1 Project Levels

Effective Date: 05/20/2019

IT projects do not come in one size, nor do they possess the same level of complexity. To support effective and cost-efficient execution of USAID IT projects, USAID defines two levels of projects based on lifecycle cost of the investment implemented by the project. The level of a project will determine the project oversight structure, the required artifacts, and the number of phase gates. The phase gate is a project management technique that reviews the end of the phase of the project. It is important to create such a review to make important decisions prior to continuing on to the succeeding phase, ending the project, or continuing but implementing some modifications.

- **Level 1 Projects**: A project is classified as Level 1 if the lifecycle cost for five years is under $10 million.

- **Level 2 Projects**: A project is classified as Level 2 if the lifecycle cost for five years is $10 million or more.

While the lifecycle cost is the primary criterion in determining the project level, the CIO has discretion to assign a different level to a project, based on criteria beyond lifecycle cost. In addition to the lifecycle cost, the factors the CIO may consider in assigning a level to a project includes:

- **Mission impact**: If an information system to be delivered is a mission-critical system, the CIO can classify the project as Level 2 even if the lifecycle cost is less than $10 million. For example, a project with the planned lifecycle cost of $7 million would have been a Level 1 project. But if the project involves a mission-critical system Agency IT project that has huge potential impact on the Agency, the CIO can classify the project as Level 2.

- **System complexity**: If an information system to be delivered by the project has high complexity, the CIO can classify the project as Level 2 even if the lifecycle cost is less than $10 million. For example, a project with the planned lifecycle cost of $5 million would have been a Level 1 project. But if it is a highly complex system (*e.g.*, involving integration with several enterprise systems), the CIO can elevate the project to Level 2 and thus provide close oversight for the project.

- **Significant information-security concern**: If a system to be delivered by the project has potentially major security exposure or concerns, the CIO can classify the project as Level 2.

The **USAID IT Project Management Guide** provides more detailed information about project levels and associated requirements.

509.3.7.2 IT Project Governance

Effective Date: 05/20/2019

IT project-governance is the Agency's method for establishing internal IT standards and accountability. It outlines formal, structured, standardized evaluation and certification procedures for the acceptance of an IT project solution and supporting deliverables, as well as the project's movement through its lifecycle.

For Level 1 projects, the M/CIO's oversight is provided through CORs and/or direct-hire Project Managers. The CORs/Project Managers identified are responsible for ensuring IT projects follow the Agency IT project management process and guidance, as described in the **USAID IT Project Management Guide**. M/CIO/IPM will conduct periodic audits of selected projects overseen by CORs and/or direct-hire Project Managers. M/CIO must provide direct oversight for Level 2 projects. The **USAID IT Project Management Guide** provides detailed information about the required documentation, checkpoints, and reporting requirements for IT projects.

a. System-Development Lifecycle Frameworks

USAID's system-development life-cycle (SDLC) frameworks provide activities and deliverables to guide IT projects from initiation through deployment.

USAID maintains two SDLC frameworks, one based on the traditional *waterfall* framework and the other based on an *agile* framework. Generally, IT infrastructure projects follow the waterfall framework and software development projects follow the

agile framework. Please refer to the Framework Selection section of the **USAID IT Project Management Guide** for descriptions of the two frameworks and information on selecting the appropriate one. All IT projects must adhere to one of these two frameworks. The project level and the SDLC framework are assigned at the time of CIO approval of the acquisition.

b. Information-Assurance

M/CIO/IA maintains the policy for IT security and determines information-security requirements for an IT project. The Information-Assurance Policy can be found in **ADS 545**.

It is important that the project sponsor and the COR/Project Manager incorporate implementation of the Agency IT security requirements into planning considerations, including the cost and schedule.

c. Privacy

The Privacy Office in M/CIO/IA maintains the Agency's privacy policy. The level of Personally Identifiable Information (PII) stored within a system determines the activities and privacy artifacts that will be required during the delivery of any IT service or solution. The Agency's privacy policy is defined in **ADS 508**.

The project sponsor and the COR/Project Manager must incorporate implementation of the Agency privacy requirements into planning considerations, including the cost and schedule.

d. Records-Management

The Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD) maintains the policy for records management. If a solution to be delivered by an IT project contains official records, it must register with the National Archives and Records Administration (NARA) and provide both the System Categorization and Disposition Schedule to IRD. The Agency's records-management policy can be found in **ADS 502**.

e. Data Standards

USAID prioritizes the use of data standards outlined in the National Information Exchange Model (NIEM) and the International Aid Transparency Initiative (IATI). Although an IT project may deliver a solution that uses different or custom standards (*e.g.*, specific to a technical discipline or subject area), the solution must be able to publish its data in a manner that is compliant with NIEM and IATI and other Agency requirements found in **ADS 579, USAID Development Data**.

509.3.7.3 Additional Federal Requirements for Software Development Projects

Effective Date: 05/20/2019

There are additional Federal requirements for software development projects, including incremental development and the sharing of source code.

a. Incremental Development

USAID IT projects for development of software or services must ensure adequate incremental development, *i.e.*, planned and actual delivery of new or modified technical functionality to users must occur at least every six months. For more information, refer to the **OMB Contracting Guidance to Support Modular Development**.

- M/CIO/PAD is responsible for tracking the use of incremental development by USAID software development projects that are part of major IT investments.

- M/CIO/PAD must conduct the analysis of the cost/schedule baselines and status for IT projects that are major IT investments on a monthly basis, determine whether those projects are planning on production releases every six months or less, and determine whether those projects actually delivered.

- M/CIO/PAD reports to the CIO, on a regular basis, the assessment results of the use of incremental development by the software development projects that are part of major IT investments.

- The CIO certifies the use of incremental development in the IT Resource Statement submitted to OMB annually.

b. Sharing of Source Code

USAID IT projects may produce custom code that other Federal departments and agencies potentially could reuse. To promote the reuse of custom code produced with Federal funding and thus maximize the benefit of taxpayer dollars, OMB issued the Federal Source Code Policy (**M-16-21**). B/IO/Ms must ensure compliance with the requirements under the OMB mandate, specifically:

- CORs must ensure delivery of the custom-developed code, documentation, and other associated materials from the developer throughout the development process.

- M/CIO/ITO must develop and maintain an up-to-date inventory of enterprise code that lists all new code that is custom-developed for USAID. CORs must ensure IT projects teams provide M/CIO/ITO necessary information about custom code developed by the projects so that the code can be listed in the USAID code inventory. M/CIO/ITO is also responsible for making the USAID enterprise code inventory discoverable at **https://www.code.gov**.

The OMB mandate **M-16-21** defines several exceptions for the sharing of custom code. For example, if the sharing of the source code would create an identifiable risk, as determined by the COR for the project and approved by the CIO, to Agency mission, programs, or operations, the custom code does not have to be shared. For a complete list of exceptions to the code-sharing requirements, refer to **M-16-21**.

509.3.7.4 IT Project Performance Reporting and Monitoring

Effective Date: 05/20/2019

This subsection defines the requirements for ensuring that Agency IT projects are effectively monitored for performance to ensure cost efficiency and service delivery.

a. IT Investment Performance Reporting

In addition to using the **Federal ITDB** for Agency budget reporting, the Federal ITDB serves as the mechanism for reporting the performance of the Agency's IT capital investments. The metrics for periodic updates and reporting to the ITDB may include the following:

- Investment risk;
- CIO's evaluation;
- Cost and schedule variance information; and
- Other project and activity-level information, such as system availability, customer satisfaction, *etc*.

M/CIO/PAD is responsible for collecting and reporting IT capital investment performance information to the Federal ITDB. Executive sponsors for IT capital investments are responsible for ensuring that IT capital investment performance information, in compliance with OMB requirements for their respective investments, is provided to M/CIO/PAD for collection and reporting to the Federal ITDB.

b. TechStat

TechStat is a tool used by M/CIO to review performance of IT capital investments. The TechStat tool is used for evidence-based accountability review and in-depth discussion of underperforming (*at-risk*) IT capital investments and their supporting program management documentation. A TechStat session focuses on the issues impeding the effective delivery of IT service, product functionality, or factors contributing to the inability to stay on schedule or budget.

The objective of TechStat is to determine a set of corrective actions to address issues with the investment to enhance performance. In some cases, however, the TechStat may result in a decision to terminate funding or discontinue the project altogether, as appropriate.

Additionally, the CIO must hold an automatic TechStat for any IT capital investment that has received a *Red* CIO evaluation (*e.g.*, high risk rating) for three consecutive reporting periods. The TechStat review goals include a realistic assessment of the investment's performance and health and the identification of necessary corrective actions. In each TechStat session, the TechStat Team from M/CIO and the Executive Sponsor, as well as the Project Manager/COR for the investment/project, work together to carefully examine program data, with a focus on problem solving that will lead to concrete actions to improve overall performance.

The Project Manager or System Owner (SO), in support of the Executive Sponsor, is responsible for providing any requested project information to the M/CIO TechStat Team. The TechStat Team is responsible for conducting the analysis of the submitted information, managing the logistics of the TechStat, coordinating the ITSS meeting to review the investment, and documenting the outcomes.

The ITSS is responsible for reviewing the findings presented by the TechStat Team and providing input to the CIO.

The details of the TechStat Process can be found in the **USAID TechStat Process document**.

509.3.8 IT Portfolio Evaluation and Optimization

Effective Date: 05/20/2019

The USAID IT portfolio consists of the following:

- **Agency IT equipment** - Includes all IT equipment procured by USAID in support of the Agency's operations. This includes, but is not limited to, computers (GFE laptops and desktops), computer monitors, mobile phones, tablets, printers, scanners, fax machines, and infrastructure equipment (router, switch, hub, server, firewall, encrypter, *etc*.);

- **Agency information systems** - Includes any information system used or operated by USAID, by a USAID contractor, or by another organization on behalf of USAID; and

- **Agency IT services provided by another organization** - Include IT services operated by other organizations that are within the scope of this ADS chapter. The service may be paid for by USAID or may be provided for free. For example, HRConnect is an IT service provided by the Department of Treasury and the use of HRConnect by USAID employees is paid for by the Agency. Another example of Agency IT services is max.gov, a free data collection and collaboration tool provided by OMB. Subscription to an online service provided by another organization (*e.g.*, subscription to ArcGIS) is also a type of IT service to be included in the Agency IT portfolio.

The USAID IT portfolio must be evaluated and optimized on an ongoing basis to ensure effectiveness and cost-efficiency of the IT investments and identify gaps in IT capabilities. Changes in Agency business needs and priorities, as well as the changes in technology, also drive the need for ongoing IT portfolio evaluation and optimization.

509.3.8.1 IT Asset and System and Service Inventories

Effective Date: 05/20/2019

To support the ongoing IT portfolio evaluation and optimization, the Agency must maintain complete and up-to-date IT asset and system and service inventories:

- **IT Asset Inventory**: A repository that includes information about USAID IT equipment.

- **Agency System and Service Inventory**: A repository that includes information about Agency information systems and IT services used by USAID but provided by other organizations.

Upon request for IT asset and system/service information by the CIO, each B/IO/M must provide the latest information, including the cost of the IT equipment, information systems, or services used by the B/IO/M that are within the scope of this ADS chapter. Heads of the B/IO/Ms are responsible for ensuring that the latest information about IT equipment, information systems, and IT services is provided to M/CIO upon request.

When requested, each IT Liaison in a B/IO must collect IT equipment, system, and service information for the B/IO and submit the information to M/CIO. Executive Officers (EXOs) at USAID overseas Missions must support the IT Liaisons for their Regional Bureaus in collecting Mission inventory information for submission to M/CIO (see **ADS 547** for additional guidance on IT asset inventory).

M/CIO/ITO is responsible for maintaining an Agency IT asset inventory. M/CIO/IPM is responsible for maintaining an online Agency IT system and service inventory.

The Agency IT system and service inventory serves as an IT solution clearinghouse for the Agency. For each information system or IT service included in the Agency IT system and service inventory, the following information, at a minimum, must be provided:

- Name,

- Description,

- Owning organization,

- Name and contact information for the SO, and

- Security Assessment and Authorization (SA&A) status.

In addition to IT asset and system and service inventories, M/CIO must maintain an inventory of data centers, and maintain a strategy to consolidate and optimize data centers.

509.3.8.2 Review of the Agency's IT Portfolio

Effective Date: 05/20/2019

The IT portfolio review is a key activity in the management of the Agency's IT resources. The USAID IT portfolio review follows the requirements established by OMB for the PortfolioStat Process. Performed by the CIO, the review has the following goals:

- Develop/maintain a comprehensive and in-depth understanding of all IT investments made by USAID in support of the Agency's operations;

- Discover opportunities to improve the Agency's IT investment portfolio by reducing suboptimal IT investments through consolidation, modernization, or decommissioning, and by preventing, detecting, and correcting shadow or hidden IT created, procured, managed, or maintained by B/IOs;

- Identify gaps in business capabilities to support the prioritization of future IT investments; and

- Support the management of information security and privacy risks associated with the Agency IT investments.

The IT portfolio review includes the following activities:

- Evaluation of each significant IT investment including the business function and value, the cost to operate and maintain (O&M), information security and privacy risks, technology platform, *etc.*; and

- Assessment of the alignment of each significant IT investment with the federal technology strategy and initiatives, the Agency ITSP, and the Agency Enterprise Architecture, including the ETR.

The CIO is responsible for leading the Agency IT portfolio review by using a data-driven approach. The CIO must engage, wherever appropriate, key stakeholders such as Executive Sponsors, system owners, and heads of B/IOs in the Agency IT portfolio review process. As a result of the Agency IT portfolio review:

- M/CIO/IPM must develop/update the Agency IT system decommissioning plan to identify and retire obsolete systems and/or reduce duplication and waste in the Agency's IT investments;

- M/CIO/IPM must update the **USAID ITSP** and/or the **ETR** to address the opportunities identified for IT portfolio optimization and the gaps in business capabilities discovered during the IT portfolio review process; and

- M/CIO/IA must update the Agency's enterprise risk-management strategy and plan to address various risks associated with IT investments, such as information-security and privacy risks.

The CIO must conduct a review of the Agency's IT portfolio at least once a year. IT Liaisons in B/IOs are responsible for leading the review of each B/IO's IT portfolio with the support of M/CIO/IPM. The goal of the B/IO IT portfolio review is to identify potential opportunities for reducing suboptimal IT investments and discover key gaps in business capabilities required to support the Agency's mission and the B/IO's operations.

The head of each B/IO must conduct an IT portfolio review at least once a year, unless they have obtained a waiver from the CIO. The results of the B/IO IT portfolio review serve as input to the review of the Agency's IT portfolio led by the CIO. The CIO has the discretion to select B/IOs for in-depth review, and to mandate optimization of the Operating Units' IT portfolios.

509.3.8.3 System Decommissioning

Effective Date: 05/20/2019

System decommissioning is the termination of an IT system's operations. Decommissioning is a key activity in the management of the Agency's IT portfolio and is critical to improving the effectiveness of IT support, optimizing the Agency's IT capital investments, and maintaining updated technology.

Often as a result of the IT portfolio review, each IT system is analyzed and a disposition of the system is recommended with one of the following options:

- Maintain the current status by continuing to operate the system without major change,

- Modernize or enhance the system to address the issues identified in the in-depth analysis, or

- Retire and decommission the system.

The CIO makes the decision to decommission an IT system, in consultation with the SO. In addition, based on the recommendation of the CISO or SAOP, the CIO can make the decision to terminate/decommission an IT system, including if it is determined the system has unacceptable risk exposure in information security or privacy and the risk exposure is too difficult or too expensive to mitigate. The SO is responsible for funding the decommissioning activities.

Decommissioning activities may consist of the following steps:

- Establishing an execution plan for decommissioning the identified system.
- Communicating the decommissioning decision, timeline, and the replacement system, if any, to the user community and other key stakeholders.
- Performing migration activities if the business functions will be supported by another system.
- Conducting training for the user community if a new system is deployed to replace the system being decommissioned. Training for the new system must be provided before the old system is terminated to minimize negative impact on Agency operations
- Terminating the system, archiving systems data, and disposing of equipment in accordance with federal guidelines.
- Performing a post-decommissioning review to document lessons learned.

For information about the system decommissioning process, roles, responsibilities, and information on system ownership, data migration and record keeping requirements, please refer to the **Operation and Maintenance of USAID's Information Technology Infrastructure and Systems Program Application Decommissioning Process Standard Operating Procedure (SOP)**.

509.3.9 Information Technology Workforce

Effective Date: 05/20/2019

To manage IT as a strategic resource, the Agency must develop and maintain a capable IT workforce.

The CHCO must work with the CIO to:

- Develop and maintain a set of competency requirements for the Agency's IT workforce, including IT Specialists; Program Managers; information-security, privacy, and IT acquisition staff; and
- Develop and maintain a current workforce planning process to ensure that the Agency can
  - Anticipate and respond to changing mission requirements,
  - Maintain workforce skills in a rapidly developing IT environment, and
  - Recruit and retain the IT talent needed to accomplish the Agency's mission.

The CHCO must also work with the CIO to:

- Ensure that the IT workforce, which supports the acquisition, delivery, management, maintenance, and use of information resources, has the appropriate knowledge and skills to facilitate the achievement of the portfolio's performance goals and, further, evaluate the extent to which the Agency's executive-level workforce has appropriate information and technology-related knowledge and skills;

- Implement innovative approaches to workforce development training, including cross-functional training, rotational development and assignments, and effective training and education methods used by the private sector, to maintain and enhance skills or obtain additional skills;

- Ensure that the SAOP is involved in assessing and addressing the hiring, training, and professional-development needs of the Agency with respect to privacy;

- Ensure that hiring managers take advantage of flexible hiring authorities for specialized positions, as established by the Office of Personnel Management (OPM);

- Assess annually the requirements established for Agency personnel regarding IT management knowledge and skills;

- Assess annually the extent to which Agency personnel meet IT management knowledge and skill requirements;

- Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies; and

- Report annually to the Administrator on progress made in improving the IT workforce capabilities.

B/IO/Ms must ensure that the IT staff within their B/IO/Ms meets the competency requirements defined by the CIO and the CHCO and work with the CIO and the CHCO in planning, hiring, training, and developing the IT staff.

509.4 MANDATORY REFERENCES

509.4.1 External Mandatory References

Effective Date: 05/20/2019

a. **41 U.S.C 2308, Modular Contracting for Information Technology**

b. **44 U.S.C. Chapter 35, Subchapter II, Information Security**

c. **Clinger-Cohen Act**

d. Department of State and USAID Joint Strategic Plan, FY 2018-2022

e. E-Government Act

f. Executive Order, Enhancing the Effectiveness of Agency Chief Information Officers, May 15, 2018

g. FAR Part 7, Acquisition Planning

h. FAR Part 10, Market Research

i. Federal Cybersecurity Workforce Assessment Act

j. Federal Information Security Management Act (FISMA) of 2002

k. Federal Information Security Modernization Act (FISMA) of 2014

l. Federal Information Technology Acquisition Reform Act (FITARA)

m. GPRA Modernization Act of 2010

n. M-12-10, Implementing PortfolioStat

o. M-13-02, Improving Acquisition through Strategic Sourcing

p. M-13-13, Open Data Policy – Manage Information As an Asset

q. M-13-23, Appendix D to Circular A-123, Compliance with the Federal Financial Management Improvement Act

r. M-15-14, Management and Oversight of Federal Information Technology

s. M-16-02, Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops

t. M-16-12, Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing

u. M-16-15, Federal Cybersecurity Workforce Strategy

v. M-16-19, Data Center Optimization Initiative (DCOI)

w. M-16-20, Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services

x. M-16-21, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software

y. M-16-24, Role and Designation of Senior Agency Officials for Privacy

z. Paperwork Reduction Act

aa. Pub. L. 114-210, MEGABYTE Act of 2016, July 29, 2016

ab. OMB Circular No. A-11, Preparation, Submission, and Execution of the Budget

ac. OMB Circular No. A-130, Manage Information as a Strategic Resource

ad. OMB Contracting Guidance to Support Modular Development

ae. OMB Memorandum, Guidance for Specialized Information Technology Acquisition Cadres

af. OMB Memorandum, Transforming the Marketplace: Simplifying Federal Procurement to Improve Performance, Drive Innovation, and Increase Savings

509.4.2 Internal Mandatory References

Effective Date: 05/20/2019

a. AAPD 16-02, Clauses and Special Contract Requirements for Facilities Access, Security, and Information Technology (IT) (Class Deviations M/OAA-DEV-FAR-18-2c and M/OAA-DEV-AIDAR-18-2c)

b. ADS 101, Agency Program and Functions

c. ADS 103, Delegations of Authority

d. ADS 201, Program Cycle Operational Policy

e. ADS 300, Agency Acquisition and Assistance (A&A) Planning

f. ADS 302, USAID Direct Contracting

g. ADS 304, Selecting the Appropriate Acquisition and Assistance (A&A) Instrument

h. ADS 508, Privacy Program

i. ADS 540, USAID Development Experience Information

j. ADS 545, Information Systems Security

k. ADS 545mbd, Rules of Behavior for Users

l. ADS 547, Property Management of Information Technology (IT)

m. ADS 547maa, Limits on Custom-Developed Software

n. ADS 549, Telecommunications Management

o. ADS 578, Information Quality Guidelines

p. ADS 579, USAID Development Data

q. ADS 620, Financial Management Principles and Standards

r. ADS 629, Accounting for USAID-Owned Property and Internal Use Software

s. Operation and Maintenance of USAID's Information Technology Infrastructure and Systems Program Application Decommissioning Process SOP

t. USAID Acquisition Regulation (AIDAR)

u. USAID IT Purchase Guidance

509.5 ADDITIONAL HELP

Effective Date: 05/20/2019

There are no additional help documents for this chapter.

509.6 DEFINITIONS

Effective Date: 04/12/2021

See the **ADS Glossary** for all ADS terms and definitions.

Adequate Incremental Development
The principle that, for the development of software or services, the delivery of new or modified technical functionality to users should take place at least every six months. (**Chapter 509**)

Agency Information System
Includes any information system used or operated by the Agency, or by a contractor of the Agency, or by another organization on behalf of the Agency. (**Chapter 509**)

Core Financial System

The system of record that maintains all transactions that result from financial event; may perform all financial functions, including management of the General Ledger, funds, payments, receivables, and costs. (**OMB Circular A-123 Appendix D**) (**Chapter 509** and **620**)

Enterprise Architecture
(i) a strategic information asset base that defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and, (iv) the transitional processes for implementing new technologies in response to changing mission needs; and includes – (i) a baseline architecture; (ii) a target architecture; and, (iii) a sequencing plan (44 U.S.C. § 3601). (**Chapter 509**)

Financial Management System
Includes the core financial systems and the financial portions of mixed systems necessary to support financial management. (**OMB Circular A-123 Appendix D**) (**Chapter 509** and **620**)

Information System
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.] Source: NIST: Key Glossary of Information Security Terms. (**Chapter 509**)

Information Technology (IT)
Includes the following:

a. Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are 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; where

b. Such services or equipment are “used by an Agency” if used by the Agency directly or if used by a contractor under a contract with the Agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

c. The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support

services that support any point of the lifecycle of the equipment or service), and related resources.

d. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment. (**Chapter 509**)

Interagency Agreement
Any agreement between two Federal agencies by which one agency buys goods or services from the other, including but not limited to an agreement under the authority of FAA section 632(b), the Economy Act, the Government Management Reform Act or similar legislation, or by which one agency transfers or allocates funds to another under the authority of FAA section 632(a). (**Chapter 300, 306, 509**)

IT Investment
An expenditure of information technology resources to address mission delivery and management support. This may include a project or projects for the development, modernization, enhancement, or maintenance of a single information technology asset or group of information technology assets with related functionality, and the subsequent operation of those assets in a production environment. These investments should have a defined life cycle with start and end dates, with the end date representing the end of the currently estimated useful life of the investment, consistent with the investment's most current alternatives analysis if applicable. (**Chapter 509**)

Internet Protocol Version 6 (IPv6)
A set of specifications from the Internet Engineering Task Force (IETF) that is an upgrade and a replacement for IP version 4 (IPv4). Both refer to the standard used in addressing information systems, computers and other similar devices to facilitate the transmission and reception of information. (**Chapters 509**, **545**, and **549**)

IT Portfolio
Includes IT investments, initiatives, programs, projects, technology services, and infrastructure in support of the technology services. (**Chapter 509**)

IT Resource
Includes the following:

a. Agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of information technology;

b. Acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but

c. Does not include grants to third parties that establish or support information technology not operated directly by the Federal Government. (**Chapter 509**)

IT Staff
IT staff provide support in systems design, development, implementation, management and operation. (**Chapter 509**)

Major Information System
A system that is part of an investment that requires special management attention as defined in OMB guidance and Agency policies, a "major automated information system" as defined in 10 U.S.C. § 2445, or a system that is part of a major acquisition as defined in the OMB Circular A-11 Capital Programming Guide consisting of information resources. (**Chapter 509**)

Major IT Investment
An investment that requires special management attention as defined in OMB guidance and Agency policies, a "major automated information system" as defined in 10 U.S.C. § 2445, or a major acquisition as defined in the OMB Circular A-11 Capital Programming Guide consisting of information resources. (**Chapter 509**)

Mission-Critical System
As defined in Public Law 106-398, any telecommunications or information system used or operated by a Department or Agency, or by a contractor of a Department or Agency, or other organization on behalf of a Department or Agency, that

(A) is defined as a “national-security” system under Section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);
(B) is protected at all times by procedures established for information that has been specifically authorized under criteria established by an Executive order or an Act of Congress to be classified in the interest of national defense or foreign policy; or
(C) processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an Agency. (**Chapter 509**)

509_092623