Capital Planning and Investment Control Policy and Overview

Office of the Chief Information Officer
Capital Planning and Investment Control Team

Version 2.9

September 2023

Revision History

Date	Version	Summary of Changes	Author
09/28/2015	1.0	Updated information technology (IT) Capital Planning and Investment Control (CPIC) policy to reflect the Federal Information Technology Acquisition Reform Act (FITARA) (December 2014) and associated Office of Management and Budget (OMB) requirements. Under FITARA, this policy is now publicly available. Agencywide Documents Access and Management System (ADAMS) Accession No. ML15247A497.	Vickie Smith, OIS/PMPD/IPMB Approved by Darren Ash, OEDO/DEDCM
12/28/2015	1.1	Updated to reflect organizational changes effective November 1, 2015. ADAMS Accession No. ML15288A545.	Vickie Smith, OCIO/PMPD/IPMB Approved by Darren Ash, CIO
10/21/2016	2.0	Updated significantly to reflect new policy requirements in the revised OMB Circular A-130, “Managing Information as a Strategic Resource” (July 2016); OMB Memorandum M-16-21, “Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open-Source Software” (August 2016); and OMB Category Management Policy for Common IT. ADAMS Accession No. ML16272A383.	Vickie Smith, OCIO/PMPD/IPMB Approved by David Nelson, CIO
12/31/2017	2.1	Revised to clarify the Chief Information Officer’s (CIO’s) role in IT contracting and incremental development, make minor changes to definitions, update the major IT investment criteria, and make other minor updates. ADAMS Accession No. ML17346A193.	Leah Kube, OCIO/GEMS/PIMB Approved by David Nelson, CIO
12/31/2018	2.2	Added and updated definitions; made other minor updates.	Leah Kube, OCIO/GEMS/IPSMB Approved by David Nelson, CIO

Date	Version	Summary of Changes	Author
12/31/2019	2.3	Added and updated definitions; made other minor editorial updates.	Leah Kube, OCIO/GEMS/IPSMB Approved by David Nelson, CIO
4/28/2020	2.4	Updated IT CPIC policy to add CIO responsibilities according to Government Accountability Office report GAO-18-93, "Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities" (August 2018). These were minor updates, and some of the responsibilities already existed in Version 2.3.	Cathy Smith, OCIO/GEMS/IPSMB Approved by David Nelson, CIO
12/8/2020	2.5	Updated some formatting and definitions based on fiscal year 2021 guidance.	Lance Breeden, Sandra Valencia, OCIO/GEMS/APIB Approved by David Nelson, CIO
1/31/2022	2.6	Updated some formatting and definitions based on fiscal year 2021 guidance.	Jack Roscoe, Sandra Valencia, OCIO/GEMS/APIB Approved by David Nelson, CIO
6/21/2022	2.7	Added appendix A.	Lance Breeden, Sandra Valencia, OCIO/GEMS/APIB Approved by David Nelson, CIO
9/12/2022	2.8	Updated the Select process area to include information on the agency's Intake Technical Review Process.	Elizabeth Naum, Sandra Valencia, OCIO/GEMS/APIB
4/20/2023	2.9	Minor updates.	Renny Thomas, Sandra Valencia, OCIO/GEMS/APIB

Note: The U.S. Nuclear Regulatory Commission maintains detailed processes and operating procedures in separate documents to support continuous refinement of the agency's maturing investment management. This document sets forth the CPIC policy and gives an overview of CPIC processes.

Contents

Background and Authorities

Capital Planning and Investment Control (CPIC) for information technology (IT) investments refers to "a decision-making process that ensures IT investments integrate strategic planning, budgeting, procurement, and management of IT in support of agency missions and business needs."[1] The Clinger-Cohen Act of 1996 (CCA) (Public Law 104-106, formerly known as the IT Management Reform Act of 1996) requires Federal agencies to use disciplined CPIC processes to acquire, use, maintain, and dispose of IT assets. Although other laws (e.g., the Paperwork Reduction Acts of 1980 and 1995, Government Performance and Results Act of 1993 (GPRA), GPRA Modernization Act of 2010 (GPRAMA), and Federal Acquisition Streamlining Act of 1994) also require agencies to develop and implement a disciplined process to maximize the value of IT investments while balancing risks, the CCA went a step further by mandating a specific, more rigorous methodology for managing IT investments that integrates IT capital planning with other agency processes.

Specifically, the CCA mandates that agencies implement CPIC processes to do the following:

- Provide for the selection, control, and evaluation of agency IT investments.
- Integrate with the processes for budget, financial, and programmatic decision-making.
- Include minimum criteria for whether to undertake an IT investment.
- Identify IT investments that would result in sharing of benefits or costs with other Federal agencies or State or local governments.
- Provide means for quantifying the net benefits and risks of IT investments.
- Allow for senior management to obtain timely information on an investment's progress.

The Federal Information Technology Acquisition Reform Act (FITARA), enacted on December 19, 2014, established additional requirements. The Office of Management and Budget (OMB) issued guidance on implementing FITARA in Memorandum M-15-14, "Management and Oversight of Federal Information Technology," dated June 10, 2015. FITARA strengthens the CCA by empowering Federal Chief Information Officers (CIOs) with increased oversight for (1) budget planning, (2) governance structures, (3) portfolio risk management, (4) hiring practices within IT offices, (5) data center consolidation planning and execution, and (6) reporting of progress and metrics to the OMB. Building on the CPIC requirements of the CCA, FITARA establishes the Common Baseline for IT Management, which defines the roles and responsibilities of the CIO and other senior agency officials while ensuring that the CIO retains accountability.

To assist agencies in meeting CCA and FITARA requirements, the OMB issued (most recently in 2022) the document "IT Budget—Capital Planning Guidance" as part of OMB Circular A-11, "Preparation, Submission, and Execution of the Budget," and OMB annually provides its submission supplement, the yearly Submission Overview, to help agencies implement CPIC processes and meet requirements for reporting to Congress. OMB Circular A-130, "Managing Information as a Strategic Resource," dated July 27, 2016, provides additional guidance for implementing CPIC and FITARA requirements. The OMB updates these circulars based on current, relevant statutes and executive orders.

[1] The Office of Management and Budget (OMB) provides this definition in the "Integrated Data Collection Common Definitions." See 40 U.S.C. 11302 for statutory requirements.

As part of FITARA, the OMB has also issued the category management policy in a series of memoranda, including the following:

- OMB Memorandum M-16-02, “Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops,” dated October 16, 2015

- OMB Memorandum M-16-12, “Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing,” dated June 2, 2016

- OMB Memorandum M-16-20, “Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services,” dated August 4, 2016

On August 8, 2016, the OMB also issued Memorandum M-16-21, “Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open-Source Software.” The CCA, FITARA, and associated OMB policy, circulars, and guidance serve as the basis for CPIC policy, processes, and procedures at the U.S. Nuclear Regulatory Commission (NRC).

Purpose

This document sets forth the NRC’s CPIC policy. It establishes the business rules and guidelines for consistency and compliance in executing the NRC CPIC processes and procedures, including the procurement of IT assets. This document contains updates that reflect FITARA, OMB Circular A-130, the OMB’s category management policy, and OMB Memorandum M-16-21 requirements; therefore, it supersedes all previous versions of the NRC’s CPIC policy.

This document also gives a brief overview of the NRC CPIC processes. It is worth noting that CPIC processes and procedures are continuously evaluated and refined; therefore, the NRC maintains separate documents on the detailed processes and procedures. This allows for timely updates and implementation and is consistent with best practices. It also supports the NRC’s goal of continuously maturing its IT investment management practices to achieve an IT portfolio that leverages IT for strategic outcomes in support of the NRC’s mission.

Definitions

The definitions in this section lay the foundation for, and build better understanding of, the CPIC policy and processes.

Adequate incremental development refers to the planned or actual delivery of new or modified technical functionality to users at least every 6 months during the development of software or services, which must be identified in OMB reports.

Agile software development is a software development approach under which requirements and solutions evolve through the collaborative effort of self-organizing and cross-functional teams and their customers or end users. It advocates adaptive planning, evolutionary development, early

delivery, and continual improvement, and it encourages rapid and flexible response to change. The use of agile software development is expected, although it is no longer broken out in OMB guidance.

Alternatives analysis is a method for assessing the various options for meeting the performance objectives of an investment; it includes assessment of the return on investment of each option. The analysis is performed before the initial decision to implement a solution, and is updated periodically, as appropriate, to capture changes in the context for an investment decision. These terms refer to best practices outlined in the Capital Programming Guide in Section I.4, “Alternatives to Capital Assets,” and Section I.5.1, “Evaluate Asset Options.”

Note: Alternatives analysis shall be performed for investments with projects in the planning stage or the development, modernization, and enhancement (DME) stage, whereas strictly operational investments require operational analyses (OAs) until a decision is made to reevaluate them or to resume DME.

Baseline refers to the approved work breakdown structure, costs, schedule, and performance goals for a given investment. OMB Memorandum M-10-27, “Information Technology Investment Baseline Management Policy,” dated June 28, 2010, provides additional information on baselines and baseline management.

Benefit-Cost Analysis (BCA) refers to the recommended technique to use in a formal economic analysis of Government programs or projects. OMB Circular A-94, “Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs,” contains guidance for performing a BCA.

Capital Programming refers to an integrated process within an agency that focuses on the planning, budgeting, procurement, and management of the agency’s portfolio of IT capital investments to achieve the agency’s strategic goals and objectives with the lowest overall cost and least risk.

CIO Evaluation refers to the CIO’s best judgment of the current level of risk for an investment relative to its ability to accomplish its goals (40 U.S.C. 11315(c)(2)). The evaluation should be informed by (1) risk management, (2) requirements management, (3) contractor oversight, (4) historical performance, (5) human capital, (6) Other factors (CPIC, EA, Records Officer), and Cybersecurity (CSOT),) that the CIO deems important to forecasting future success. Each evaluation should include a narrative to explain the rating; this is particularly important when the rating has changed since the last evaluation.

CIO TouchPoints are direct one-on-one discussions between the NRC’s CIO and the members of the integrated project team (IPT) for a major IT investment (including IT project managers, subject-matter experts (SMEs), business process owners, information system security officers, system owners, and others as appropriate), especially IT project managers executing projects under the investment.

Cloud Computing refers to a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing promotes availability. It comprises five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), three service models (cloud software as a service (SaaS), cloud platform as a service (PaaS), and cloud infrastructure as a service (IaaS)), and four deployment models (private

cloud, community cloud, public cloud, and hybrid cloud). Key enabling technologies include fast wide-area networks; powerful, inexpensive server computers; and high-performance virtualization for commodity hardware.

Cloud First Policy refers to the OMB's Cloud First policy, also known as the Federal Cloud Computing Strategy, which was launched in December 2010. This policy is intended to accelerate the Government's realization of the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.

Note: The Federal Cloud Computing Strategy requires agencies to do the following:

- *Evaluate their technology sourcing plans to include consideration and application of cloud computing solutions as part of the budget process.*
- *Seek to optimize the use of cloud technologies in their IT portfolios to take full advantage of the benefits of cloud computing to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize costs.*
- *Default to cloud-based solutions when evaluating options for new IT deployments, if a secure, reliable, cost-effective cloud option exists.*
- *Continually evaluate cloud computing solutions across their IT portfolios, regardless of investment type or life-cycle stage.*

The Cloud First policy is supported by the Cloud Smart strategy, which is intended to accelerate agency adoption of cloud-based solutions. The Cloud Smart strategy is founded on three pillars of successful cloud adoption: security, procurement, and workforce. These elements embody the interdisciplinary approach to IT modernization that the Federal enterprise needs to provide greater return on its investments, enhanced security, and higher quality services to the American people.

Commodity IT refers to a category of back-office IT services used by most, if not all, agencies (e.g., infrastructure and asset management, email, hardware and software acquisition, and help desks). Commodity IT is related to the OMB's PortfolioStat initiative; it plays a key role in a CIO-led business approach to the delivery of IT infrastructure, enterprise IT, and administrative and business systems that encourages agencies to pool purchasing power across their entire organization, by both providing and using shared services instead of implementing independent services with similar functions. This approach aims to eliminate duplication, rationalize each agency's IT investments, and drive down costs.

There are three categories of Commodity IT:

(1) Enterprise IT: email; collaboration tools; identity and access management; IT security (apart from identity and access management); and web hosting, infrastructure, and content

(2) IT Infrastructure: desktop systems, mobile devices, mainframes and servers, and telecommunications

(3) Business Systems: financial management, human resources management, grant-related Federal financial assistance, and grant-related transfer to State and local governments

Cost is defined in Statement of Federal Financial Accounting Concepts No. 1, "Objectives of Federal Financial Reporting," dated September 2, 1993, as "the monetary value of resources used." It is defined more specifically in Statement of Federal Financial Accounting Standards (SFFAS) No. 4, "Managerial Cost Accounting Concepts and Standards," dated July 31, 1995, as "the monetary value of resources used or sacrificed or liabilities incurred to achieve an objective, such as to acquire or produce a good or to perform an activity or service." Depending on the transaction, cost may be charged to operations immediately (i.e., recognized as an expense of the period), or it may be charged to an asset account for recognition as an expense of subsequent periods. In most contexts within SFFAS No. 7, "Accounting for Revenue and Other Financing Sources and Concepts for Reconciling Budgetary and Financial Accounting," dated May 10, 1996, "cost" is used synonymously with "expense."

Cost Avoidance (as defined in OMB Circular A-131, "Value Engineering," dated December 26, 2013) refers to an immediate action that will decrease costs in the future. An example of a cost avoidance action is an engineering improvement that increases the mean time between failures and thereby decreases operation and maintenance costs.

Cost Savings (as defined in OMB Circular A-131) refers to the reduction in actual expenditures to achieve a specific objective.

Development, Modernization, and Enhancement (DME) refers to projects and activities that lead to new IT assets or systems, or that change or modify existing IT assets or systems, to substantively improve capability or performance, meet legislative or regulatory requirements, or fulfill agency leadership requests. A DME activity may occur at any time during a program's life-cycle. Capital costs involved in DME may include costs of hardware and software development and acquisition; commercial off-the-shelf acquisition; Government labor; and contracted labor for planning, development, acquisition, system integration, and direct project management and overhead support.

Disposition Cost refers to the cost of retiring a capital asset (generally a system or investment) once its useful life is over or a replacement asset has superseded it; disposition costs may be included in operational activities near the end of the asset's useful life.

Earned Value Management (EVM) refers to an integrated management system that coordinates the work scope, schedule, and cost goals of a program or contract and objectively measures progress toward these goals. EVM is a tool used by program managers to (1) quantify and measure program or contract performance, (2) provide an early warning system for deviation from a baseline, (3) mitigate risks associated with cost and schedule overruns, and (4) provide a means to forecast final cost and schedule outcomes. A description of the qualities and operating characteristics of an earned value management system (EVMS) appears in American National Standards Institute/ Electronic Industries Alliance Standard 748-1998, "Earned Value Management Systems," dated May 19, 1998. Additional information on EVM is available at https://www.acq.osd.mil/asda/ae/ada/ipm/index.html.

Note: For lower cost programs and projects for which the high cost of using EVM may be prohibitive, an alternative approach must be described under risks in the program or project plan, or in a separate risk management plan, as appropriate.

Enterprise Architecture (EA) refers to an organization's documentation of the current and desired relationships among business and management processes and IT. An EA includes the rules,

standards, and system life-cycle information to optimize and maintain the environment that the agency wishes to create and maintain through its IT portfolio. An EA must contain a strategy for the agency to maintain its current state, as well as a roadmap for transition to its target environment. An EA defines principles and goals and sets a direction for the promotion of such issues as interoperability, open systems, public access, end user satisfaction, and IT security.

Note: Although this document does not establish EA standards, the selection and evaluation criteria found within should align with, and be reflected in, the NRC's target EA and Enterprise Roadmap.

Enterprise Roadmap refers to a document that describes the business and technology plan for the entire organization using EA methods. The Enterprise Roadmap provides current views, future views, and transition plans at an appropriate level of detail for all IT investments, services, systems, and programs. It also contains an IT asset inventory using the Federal Enterprise Architecture reference models, as well as other attachments or appendices giving more information on Roadmap plans for CPIC, EA, shared services, and other planning products requested by the OMB.

Federal IT Dashboard (ITDB) refers to a website (https://www.itdashboard.gov/) where Federal agencies, industry, the general public, and other stakeholders can view details of the performance of Federal IT investments. The administration and Congress use the ITDB to inform budget and policy decisions. The ITDB is also known as IT Collect.

Financial Management Systems are systems necessary to support financial management. They include automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. Examples of financial management systems include (1) core financial systems, (2) procurement systems, (3) loan systems, (4) grants systems, (5) payroll systems, (6) budget formulation systems, (7) billing systems, and (8) travel systems. OMB Circular A-127, "Financial Management Systems," dated January 9, 2009, contains additional information and guidance.

Functional/Business Sponsor refers to the agency official responsible for a program or function supported or implemented by an investment (44 U.S.C. 3501(a)(4)). The sponsor is responsible for expressing the value of the investment, ensuring its successful implementation, and providing accurate and timely data to the agency CIO and the OMB. The sponsor may (or may not) be the same person as the business process owner or SME serving on the IPT. Each major and non-major IT investment must include the name and title of the functional or business sponsor.

Information and Communication Technology (ICT) refers to IT and other equipment, systems, technologies, or processes whose principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as to any associated content. Examples of ICT include software applications, websites, videos, electronic documents, computers and peripheral equipment, information kiosks and transaction machines, telecommunications equipment, customer premises equipment, multifunction office machines, and digital signs.

Information Resource Management (IRM) Strategic Plan refers to a document that comprehensively addresses an agency's IRM. Agencies must develop and maintain their IRM Strategic Plans as required by 44 U.S.C. 3506(b)(2) and OMB Circular A-130. IRM Strategic Plans should support the Agency Strategic Plan required by OMB Circular A-11; describe how IRM activities support the agency's mission delivery area and program decisions; and ensure that IRM decisions are integrated with management support areas, including organizational planning, budget, procurement, financial management, and human resources management.

Information Security refers to all functions pertaining to the protection of Federal information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction. It includes the development, implementation, and maintenance of security policies, procedures, and controls throughout the entire information life-cycle. Information security activities should include those described in National Institute of Standards and Technology (NIST) Special Publication 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations," among which are (1) security awareness training (but not the technical infrastructure required for the delivery of training), (2) compliance reporting under the Federal Information Security Management Act, (3) development of a security policy, and (4) security audits and testing.

Note:

- *IT security should include systems that oversee agency IT needs.*
- *IT security does not include IT costs related to identity or access management systems or solutions.*
- *IT security does not include physical protection of an organization (e.g., guards, cameras, and facility protection).*

Information System refers to a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, transmission, or dissemination of information, in accordance with defined procedures, whether automated or manual.

Information Technology (IT) is defined as follows:

- IT includes any services or equipment, or interconnected systems or subsystems of equipment, that are used by an agency in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
- Such services, equipment, or systems are considered "used by an agency" if either the agency uses them directly, or a contractor uses them under a contract with the agency that requires either full or significant use of them to perform a service or furnish a product.
- IT includes computers; ancillary equipment (such as imaging peripherals and 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 related resources, procedures, and services (including provisioned services such as cloud computing and support services for any point of the equipment or service life-cycle).
- IT includes high-performance computing capabilities, including those that are not communal in nature.
- IT does not include any equipment acquired by a contractor incidentally to a contract that does not require its use.

Intake Technical Review Process refers to the process the Office of the Chief Information Officer (OCIO) uses to efficiently and effectively serve the NRC stakeholders when evaluating new

hardware and software requirements that are introduced to the NRC enterprise infrastructure for implementation.

IT Assets are any IT-related items (tangible or intangible) that have value to an organization, including, but not limited to, computing devices; IT systems, networks, and circuits; software (either installed or physical instances); virtual computing platforms (which are common in cloud and virtualized computing); related hardware (e.g., locks, cabinets, keyboards); and people and intellectual property (including software).

Note: Assets are the lowest level at which IT is planned, acquired, implemented, and operated. All IT hardware and software shall be associated with the comprising system or investment and tracked and monitored throughout its life-cycle, in accordance with the NRC's IT asset management processes.

IT Investment refers to the expenditure of IT resources to enable mission delivery and management support. An IT investment may include one or more projects for the DME or maintenance of either a single IT asset or a group of IT assets with related functionalities, or for the subsequent operation of the asset(s) in a production environment.

Note: All IT investments shall 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 recent alternatives analysis, if applicable. When an asset is essentially replaced by a new system or technology, the replacement shall be reported as a new, distinct investment, with its own defined life-cycle information.

There are five types of IT investment:

(1) **Funding Transfer Investment** refers to the portion of funding a partner agency contributes to an investment managed by another agency. The description of the investment should indicate the unique investment identifier (UII) of the managing partner's investment.

Note: As a partner agency on multiple funding transfer investments (e.g., E-Gov, line-of-business (LoB), and shared services), the NRC shall budget for and report the funding provided to each managing agency on the Agency IT Portfolio Summary that it submits to the OMB. During the Select process, funding transfer investments shall be considered in the alternatives analysis. If a funding transfer investment is not selected, the agency must provide a business justification for the solution selected instead, which must be approved by the CIO and submitted to the OMB for approval.

(2) **IT Migration Investment** refers to the costs associated with a partner agency's migration to a shared service that are not captured by the managing partner. The description of the investment should indicate the UII of the managing partner's investment.

Note: The NRC shall plan, budget for, and report the IT cost of migrating to new investments or to funding transfer investments. When migrating to a funding transfer investment, the NRC shall report the cost as an IT migration investment in the Agency IT Portfolio Summary. When migrating to a new investment that is not a funding transfer investment, the NRC shall report the cost as planning DME in the new investment's life-cycle cost table.

(3) **Major IT Investment** refers to an IT investment requiring special management attention because of its importance to the mission or function of the Government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; unusual funding mechanism; or definition as major through the agency's CPIC process. Major IT investments include all "major automated information systems" (as defined in 10 U.S.C. 2445) and all "major acquisitions" (as defined in the Capital Programming Guide) that include information resources. The OMB may work with the agency to declare IT investments as major IT investments. Agencies must consult with assigned OMB desk officers and resource management offices to determine which investments are considered "major."

(4) **Non-Major Investment** refers to any investment in the agency's IT portfolio that does not meet the definition of a major IT investment, funding transfer investment, or IT migration investment.

(5) **Standard Investment** refers to an IT infrastructure investment that has disaggregated to its discrete components, which are managed separately.

IT Program Managers and IT Project Managers are the personnel who lead the IPT for a given investment. In some cases, IT program or project managers can hold positions in other classification series; however, they must still meet the applicable Federal certification or IT program management experience requirements. Further definitions are available in the Office of Personnel Management's Job Family Standard for Administrative Work in the Information Technology Group (Series 2200 in the Federal Classification and Job Grading Systems).

IT Resources include the following:

- agency budgetary resources, personnel, equipment, facilities, and services that are primarily used in the management, operation, acquisition, disposition, or transformation of IT, or in other activity related to the IT life-cycle

- acquisitions or interagency agreements that include IT, and the services or equipment they provide

IT resources do not include grants to third parties that establish or support IT not operated directly by the Federal Government.

IT Service refers to a means of delivering IT, together with any personnel or processes of value, to facilitate outcomes that customers want to achieve without the costs and risks of ownership.

Integrated Project Team (IPT) refers to a multidisciplinary team associated with an IT investment. Each IPT is led by an IT program or project manager responsible and accountable for planning, budgeting, and procurement, as well as life-cycle management to achieve the investment's cost, schedule, and performance goals. Team skills include budgetary, financial, capital planning, procurement, user, program, architecture, EVM, security, and other skills, as appropriate.

Note: For the OMB to approve the budget for a major IT investment, its IPT must include at least the following:

- *a qualified, fully dedicated IT program/project manager*
- *a contracting specialist, if applicable*
- *an IT specialist*
- *an IT security specialist*
- *a business process owner or SME*

The IPT might also include the following:

- *an enterprise architect*
- *an IT specialist with specific expertise in data, systems, or networks*
- *a capital planner*
- *a budget contact*
- *a contracting officer's representative*
- *an information system security officer*
- *a performance specialist*

Key members of the IPT should be colocated during the most critical junctures of the program, to the maximum extent possible. Agencies should establish individual performance goals for IPT members, to hold them accountable for both individual functional goals and the overall success of the program. The IPT should be defined in a program or an IPT charter.

Interagency Acquisition refers to the use of the Federal Supply Schedules, a multiagency contract (i.e., a task order or delivery order contract established by one agency for use by multiple Government agencies to obtain supplies and services, consistent with the Economy Act, 31 U.S.C. 1535), or a Governmentwide acquisition contract (i.e., a task order or delivery order contract for IT established by one agency for Governmentwide use, operated by an executive agent, as designated by the OMB pursuant to CCA section 11302(3)).

Life-Cycle Costs are all costs, including Government full-time equivalents (FTEs), from the beginning of an investment until the end of its estimated useful life (or the composite estimated useful lifetimes of the assets within it), independent of the funding source (e.g., revolving fund, appropriated fund, working capital fund, trust fund). The Capital Programming Guide and OMB Circular A-131 contain more information about life-cycle costs.

Maintenance refers to the activity necessary to keep an asset functioning as designed during the operations and maintenance phase of an investment. Maintenance activities include, but are not limited to, operating system upgrades, technology refreshes, and security patch implementations. As defined in SFFAS No. 10, "Accounting for Internal Use Software," dated October 9, 1998, maintenance excludes activities aimed at expanding an asset's capacity or otherwise upgrading it to serve needs different from or significantly greater than those originally intended. Such activities are considered DME.

Note: Maintenance activities of notable cost or duration with predetermined start and end dates should be managed as projects and reported in the project and activity tables in section B of the Major IT Investment Update.

Managing Partner refers to the lead agency that is responsible for coordinating the implementation of a funding transfer investment. The managing partner maintains an IT shared service, with approval from agency leadership for intra-agency services and from the OMB for interagency

services. The managing partner organization, often referred to as the Program Management Office, develops, implements, and maintains financial and service models, as well as contracts with customers and suppliers, using strategic sourcing vehicles whenever practicable. The Program Management Office is responsible for the success of the IT shared service; it reports on its intra-agency shared service using the agency's own metrics, and on interagency LoBs using metrics developed by the Federal CIO Council's Shared Services Subcommittee. Managing partners are also responsible for maintaining contracts with customer agencies that allow the customer agency to terminate the contract if specified levels of service are not maintained.

Modular Development refers to the approach of delivering investments, projects, or activities of a specified capability by progressively expanding on delivered capabilities until the full capability is realized. Investments may be decomposed into discrete projects, increments, or useful segments, each of which is undertaken to develop and implement products and capabilities that form part of the overall investment. The OMB's "Contracting Guidance to Support Modular Development," dated June 14, 2012, provides more information.

Operational Analysis (OA) refers to a method of examining the ongoing performance of an operating asset and measuring it against established cost, schedule, and performance goals. An OA is by nature less structured than the performance reporting methods applied to developmental projects. It should trigger considerations of how to better meet the investment's objectives, how to reduce costs, and whether the organization should continue performing a particular function. The Capital Programming Guide contains guidance on OAs. Best practices also appear in the Government Accountability Office (GAO) report GAO-13-87, "Information Technology: Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments," issued October 2012.

Operations refers to the day-to-day management of an asset while it is in a production environment, producing the same product or providing a repetitive service. Operations include, but are not limited to, activities in data centers, help desks, operational centers, telecommunication centers, and end-user support services.

Operations and Maintenance refers to the expenses required to operate and maintain an IT asset that is operating in a production environment. It includes costs associated with operations, maintenance activities, and maintenance projects needed to sustain the asset at the current capability and performance levels. Specifically, it covers the costs of Federal and contracted labor, corrective hardware and software maintenance, voice and data communications maintenance and service, replacement of broken or obsolete IT equipment, overhead, business operations and commercial services, and asset disposal. It is also commonly referred to as "steady state."

Partner (Customer) Agency refers to the agency in an inter- or intra-agency collaboration, such as an E-Gov, LoB initiative, or Federal shared service, that contracts with and pays a managing partner for an IT shared service. While the managing partner handles major contract issues and resolves escalation items with suppliers, the partner agency may need to interact with suppliers to handle day-to-day service issues. The partner agency usually provides resources (e.g., funding, FTEs) for the management, development, deployment, or maintenance of a common solution. The partner agency is also responsible for including the appropriate line items in its own IT Portfolio Summary budget submission to reflect the amount of its contribution to each of the initiatives for which it provides resources.

Planning refers to preparing, developing, or acquiring the information needed to design an asset; assessing the benefits, risks, and risk-adjusted costs of alternative solutions; and establishing realistic cost, schedule, and performance goals for the selected alternative, before either proceeding to full acquisition or terminating the project.

Note: Before the acquisition phase can begin, planning must progress to the point where the agency is ready to commit to specific goals for the completion of the acquisition. Information-gathering activities and tools to support planning may include the following:

- *market research on available solutions (see Federal Acquisition Regulation (FAR) Part 10, "Market Research")*
- *architectural drawings*
- *engineering and design studies*
- *prototypes*

Planning may be general, for the overall investment, or it may be specific to a useful component. For investments developed or managed using an iterative or agile methodology, planning will occur throughout the entire acquisition, focusing on each iteration or sprint.

Post-implementation Review (PIR) refers to an evaluation of how successfully the objectives of an investment or project were met and how effectively the project management practices kept it on track. A PIR can be conducted after the completion of a project or at the conclusion of the implementation phase of an investment. The Capital Programming Guide contains additional details on the PIR process.

Privacy Impact Assessment (PIA) refers to the process for examining the risks and ramifications of using IT to collect, maintain, and disseminate information in identifiable form from or about members of the public. PIAs are also used to identify and evaluate protections and alternative processes to mitigate the privacy impact of collecting such information. Consistent with OMB Memorandum M-03-22, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," dated September 26, 2003, agencies must conduct and make publicly available PIAs for all new or significantly altered IT investments that administer information in identifiable form collected from or about members of the public.

Programming refers to an integrated process within an agency that focuses on the planning, budgeting, procurement, and management of a program to achieve the agency's strategic goals and objectives with the lowest overall cost and least risk.

Note: Any program that leverages IT to support its mission shall include the CIO in its programming to advise on and approve the IT aspects of the program.

Project refers to a temporary endeavor undertaken to provide a unique product or service. A project has a defined start and end point and specific objectives that, when attained, signify completion. Projects can be undertaken for the DME, disposal, or maintenance of an IT asset. Projects are composed of activities.

Note: When reporting project status, to the maximum extent practicable, agencies should detail the characteristics of "increments" under modular contracting, as described in the CCA, and the characteristics of "useful segments," as described in OMB Circular A-130.

Risk Management refers to a systematic process of identifying, analyzing, and responding to risk. It includes maximizing the probability and consequences of positive events and minimizing the probability and consequences of adverse events. Risk management should be conducted throughout the entire life-cycle of a program.

Risk Management Plan refers to a documented and approved plan, developed at the onset of an investment and maintained throughout, that specifies the investment's risk management process.

Shadow (Hidden) IT refers to IT spending that is not fully transparent to the agency CIO, and to IT resources included in a program whose primary purpose is not IT related. An example would be a grants program in which a portion of the spending goes to equipment, systems, or services that provide IT capabilities for administering or delivering the grants.

Shared Service refers to a service that one Federal organization provides to other Federal organizations that are outside the provider's organizational boundaries. Shared services may be intra-agency or interagency. There are three categories of shared services in the Federal Government:

(1) **Common Solutions**—technology or contracts that can be used by more than one Federal agency. May be Government-to-Government or citizen-to-Government.

(2) **Shared Services**—services consolidating routine or standard operations to a limited number of organizations. May use common solutions (technology or contracts) and share human resource expertise either within an agency or across agencies.

(3) **Centralized Services**—services providing a single Governmentwide location for highly standardized activities, allowing organizations and users to benefit from consistent and uniform processes.

Note: Shared commodity IT and support services are considered to be IT; associated costs must be included and reported as part of the IT Portfolio Summary.

Shared Service Provider refers to the provider of a technical solution or service that supports the business of multiple agencies using a shared architecture. For multiagency services, this is the managing partner of the investment.

TechStat Sessions are a tool for anticipating critical problems in an investment, turning around underperforming investments, or terminating investments if appropriate. Agencies report the outcomes of all TechStat sessions through the quarterly Integrated Data Collection (IDC) process.

Unique Investment Identifier (UII) refers to a persistent numeric code applied to an investment in an agency's IT portfolio that allows it to be identified and tracked across multiple fiscal years. The UII consists of a three-digit agency code linked with a unique nine-digit investment number generated by the agency. Some nine-digit numbers are reserved for the OMB to assign to funding transfer investments and may not be assigned by agencies.

Capital Planning and Investment Control Policy

All NRC IT resources shall be managed in accordance with Federal mandates, OMB requirements, and agency procedures. This policy establishes the business rules and guidelines for the management and oversight of IT resources, including FTEs, under all IT investments, except where it is stated that the rules apply only to major IT investments.

Planning, Programming, Budgeting, and Selecting

(1) All IT resources shall be planned, budgeted, executed, and reported under an approved IT investment in the NRC IT Portfolio Summary submitted to the OMB during the annual budget submissions.

(2) For each IT investment, descriptive and financial data (including data on the investment's performance and the expenditure of IT resources) must be developed and maintained to justify the budget request to the OMB and Congress.

(3) An IT investment shall be classified as a major IT investment if it meets one or more of the following OMB criteria:

- importance to the mission or function of the Government
- significant program or policy implications
- high executive visibility
- high development, operations, or maintenance costs, which the NRC defines as budget planning year costs of $10 million or more[2]
- unusual funding mechanism
- financial systems with annual cost and spending of $500,000 or more, as dictated by mandates and guidance on financial systems, such as OMB Circular A-127
- definition as major by the NRC's CPIC process

All other NRC IT investments are considered non-major or standard investments, apart from funding transfer investments and IT migration investments. The NRC is a partner agency on a number of investments managed by other agencies. These investments are considered major IT investments of the managing agencies, and the NRC shall report contributions to the managing partners in the NRC IT Portfolio Summary.

(4) During the planning, programming, and budgeting processes, all IT resources shall be identified and separated from non-IT resources to allow visibility to the CIO and the Information Technology/Information Management (IT/IM) Portfolio Executive Council (IPEC). Budgeting for IT resources in all programs (not just programs that are primarily IT-oriented) shall follow the IT budget guidance issued by OCIO and shall take place in tandem with the overall agency budget formulation process issued by the Office of the Chief Financial Officer (OCFO). The budgeting process includes defining the level of detail at which IT resources are budgeted and, in consultation with the Chief Acquisition Officer (CAO), defining

[2] The OMB establishes the criteria for a major IT investment but allows agencies to establish the dollar threshold.

processes to track planned versus actual expenditures for all transactions that include IT resources. The Chairman is regularly briefed on the status of IT investments and activities.

(5) As a co-chair of the IPEC, the CIO shall advise on and approve the IT aspects of all programs. In the case of major IT investments, more extensive involvement shall occur through monthly updates, CIO evaluations, and CIO TouchPoints.

(6) The IT budget formulation process and the annual Agency IT Portfolio Summary submission process shall ensure that the budget justification materials in the NRC's initial budget submission receive the appropriate CIO approvals and certifications and include the corresponding affirmation statements, as listed in OMB Circulars A-130 and A-11.

(7) The CIO and CFO shall define and, as the co-chairs of the IPEC, shall oversee the process by which the CIO, CFO, CAO, and Chief Human Capital Officer (CHCO) work with program leadership to plan an overall IT portfolio that efficiently and effectively leverages IT to further program and business objectives aligned with the agency's Strategic Plan.

(8) An IT investment's justification, cost, schedule, measurement indicators, and other management and technical artifacts shall describe the discrete and unique set of IT products and services it encompasses and how they contribute to the NRC mission or mission support functions. For all major IT investments, the agency shall document and report all of the above to the OMB (when requested).[3]

(9) Major IT investments shall adhere to the principles established by the OMB in Appendix 6, "Principles of Budgeting for Capital Asset Acquisitions," to the Capital Programming Guide.

(10) No two IT investments shall serve the same purpose or deliver the same discrete and unique set of products or services. If duplicative investments are identified, an alternatives analysis shall be performed, and a plan developed to eliminate the duplication and associated cost.

(11) When two or more IT investments deliver products or services through the same IT component (i.e., system or platform), the set of products or services delivered through that component by each investment shall be discrete and unique and clearly distinguishable from the products and services delivered by the other investments through the same component. In addition, there must be a consistent, reliable means of determining an equitable cost of the shared platform for each investment, to ensure accurate planning, budgeting, and reporting of the total cost of ownership of each investment.

(12) All IT investments shall 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 recent alternatives analysis, if applicable. When an asset is essentially replaced by a new system or technology, the replacement shall be reported as a new, distinct investment, with its own defined life-cycle information.

(13) Information security, privacy, records management, public transparency, and supply chain security issues must be considered for all resource planning and management activities throughout a system's development life-cycle.

[3] NRC CPIC procedures for Major IT Business Cases are based on the OMB's annual "IT Budget—Capital Planning Guidance," issued as part of OMB Circular A-11.

(14) All major IT investments shall have a committed IPT comprising the required minimum membership (as noted in the definition of IPT) and program charter. All IT projects shall have an IPT, project charter, project management plan, and schedule.

(15) Alternatives analysis shall be performed for investments with projects in the planning or DME stages. The alternatives analysis shall include both Government-provided (internal, interagency, and intra-agency) and commercially available options, as well as cloud solutions, where applicable.

(16) The alternatives analysis for a new investment shall include the Three-Step Software Solutions Analysis described in OMB Memorandum M-16-21, which addresses Federal source code policy.

(17) To strengthen understanding of the requirements for an IT service, qualitative and quantitative research methods shall be used to determine the goals, needs, and behaviors of current and prospective managers and users of the service.

(18) All acquisition planning shall adhere to the planning provisions in FAR Subpart 7.1, “Acquisition Plans,” and FAR Part 10.

(19) Planning for IT acquisitions shall substantiate the NRC’s commitment to achieving specific goals through the completion of each acquisition. Planning activities and results shall be documented, and final plans approved before the acquisition phase begins. For investments developed or managed using an iterative or agile methodology, proper planning for each iteration or sprint shall be conducted throughout the life of the investment.

(20) All IT hardware and software shall be planned, acquired, deployed, managed, and disposed of under IT investments in the NRC’s IT Portfolio Summary and in accordance with the NRC’s IT asset life-cycle management processes and procedures.

(21) In analyzing and prioritizing IT investments for selection into the agency IT portfolio, all decisions to select (acquire or develop) an information system technology or service shall be merit-based and shall consider factors including, but not limited to, the following:

- alignment to the NRC’s Strategic Plan
- ability to meet operational or mission requirements
- conformance to the current and target EA, and alignment to the Enterprise Architecture Roadmap
- total life-cycle costs of ownership and ability to sustain such costs
- performance
- security risks
- interoperability
- privacy
- accessibility

- ability to be shared or reused
- resources required to switch vendors to avoid being “locked in”
- availability of high-quality support at a reasonable cost

(22) The decision to improve, enhance, or modernize an existing IT investment or to develop a new IT investment shall be based on an alternatives analysis that covers both Government-provided (internal, interagency, and intra-agency, where applicable) and commercially available options, from which the option offering the best value to the Government shall be selected.

(23) Preference shall be given to using available and suitable Federal information systems, technologies, or shared services or information-processing facilities, or to acquiring open-source or commercially available off-the-shelf software or technologies, over developing or acquiring custom or duplicative solutions.

(24) Decisions to acquire custom or duplicative solutions must be justified by their overall life-cycle cost-effectiveness or their ability to meet specific high-priority mission or operational requirements.

(25) The security levels of information systems shall be commensurate with the risk that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of the information they contain, consistent with NIST standards and guidelines.

Acquiring Information Technology and Services

When acquiring IT and IT services, the NRC shall adhere to the following:

- all relevant Federal mandates, such as 41 U.S.C. 2308, “Modular Contracting for Information Technology”
- OMB policy, including but not limited to the category management policies for improving the acquisition and management of common IT, such as the following:
  - laptops and desktops (OMB Memorandum M-16-02)
  - software licensing (OMB Memorandum M-16-12)
  - mobile devices and services (OMB Memorandum M-16-20)
- the FAR, including the planning provisions in Subpart 7.1 and Part 10 to be implemented before an acquisition
- NRC Management Directive 11.1, “NRC Acquisition of Supplies and Services,” dated May 9, 2014

During the acquisition process, all of the above must be referenced and applied as appropriate. This includes, but is not limited to, the following policy guidelines:

(1) Develop a thorough benefit-cost analysis of all procurement requirements based on market research, including an alternative analysis.

(2) Effectively use 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.

(3) Conduct definitive technical, cost, and risk analyses of alternative design implementations, considering, for example, the full life-cycle costs of IT products and services, which include but are not limited to planning, analysis, design, implementation, sustainment, maintenance, re-competition, and retraining costs, scaled to the size and complexity of individual requirements.

(4) When developing planned information systems, consider existing Federal contract solutions or shared services available from within the same agency, from other agencies, or from the private sector, to avoid duplicative investments.

(5) Initiate development of new information systems, or of custom solutions to improve existing information systems, only when no existing private-sector or Government source can efficiently meet the need, taking into account long-term sustainment and maintenance.

(6) Structure acquisitions for major IT investments into useful segments, each of narrow scope and brief duration, to reduce risk, promote flexibility and interoperability, increase accountability, and better match mission needs with current technology and market conditions.

(7) To the extent practicable, award modular contracts for IT, including orders for increments or useful segments of work, no more than 180 days after issuing the solicitation. If an award cannot be made within 180 days, consider canceling the solicitation. The IT acquired should be delivered no more than 18 months after the solicitation was issued.

(8) Align IT procurement requirements with the agency's strategic goals.

(9) Promote innovation in IT procurements; in particular, conduct market research to maximize the use of innovative ideas.

(10) Include requirements for security, privacy, accessibility, records management, and other relevant considerations in solicitations.

(11) Ensure that the CIO reviews and approves all acquisition strategies, plans, and requirements (as described in FAR Part 7, "Acquisition Planning") and all interagency agreements (such as those used to support purchases through another agency) that involve IT. These approvals shall consider the following factors:

- alignment with mission and program objectives in coordination with program leadership
- appropriateness with respect to the mission and business objectives supported by the NRC's IRM Strategic Plan
- inclusion of innovative solutions
- appropriateness of contract type for IT-related resources
- appropriateness of IT-related portions of statement of needs or statement of work

- ability to deliver functionality in short increments
- inclusion of Governmentwide IT requirements, such as information security
- opportunities to migrate from and retire end-of-life software and systems

(12) Consistent with the FAR, include in contracts for custom software development provisions that reaffirm the right to reuse the software throughout the Federal Government.

(13) Enter all acquired IT hardware and software into the NRC's IT asset inventory and management tools.

Information Technology Investment Design and Management

The NRC shall, to the extent practicable and financially responsible, implement the following requirements:

(1) Information systems and processes shall support and maximize interoperability and access to information, where appropriate, by using documented, scalable, and continuously available application programming interfaces and open machine-readable formats.

(2) Information systems and technologies must facilitate interoperability, application portability, and scalability across networks of heterogeneous hardware, software, and communications platforms.

(3) When ICT is developed, procured, maintained, or used, it must be in compliance with Title 36 of the *Code of Federal Regulations* 1194.1, "Standards for Section 508 of the Rehabilitation Act."

(4) In designing, developing, integrating, or implementing IT solutions, the practices and architecture must conform to the NRC IT/IM Technical Standards.

(5) All information life-cycle processes and stages, including the design, development, implementation, and decommissioning processes for information systems, must fully incorporate electronic records management (ERM) functions, policies, and retention and disposition requirements or have electronic recordkeeping mitigation strategies in place. Laws and regulations under the National Archives and Records Administration (NARA) require agencies to manage information throughout its life-cycle, regardless of the media. This applies particularly to Internet resources, including storage solutions and cloud-based services in the form of software as a service, platform as a service, or infrastructure as a service.

(6) A PIA and security impact assessment must be performed up front, and the appropriate security planned, budgeted, and built in at the start of the project.

(7) IT investments shall use an EVMS and Integrated Baseline Review, when appropriate, as required by FAR Subpart 34.2, "Earned Value Management System." When an EVMS is required, agencies must have a documented process for accepting a contractor's EVMS. When an EVMS is not required, a baseline validation process must be implemented as part of an overall investment risk management strategy consistent with OMB guidance.

(8) All IT development projects shall appropriately implement incremental development and modular approaches, as defined in the OMB's "Contracting Guidance to Support Modular Development."

(9) Maintenance activities of notable cost or duration with predetermined start and end dates should be managed as projects. In the case of major IT investments, the project and activity tables in section B of the Major IT Investment Update shall track, monitor, and report the cost and schedule.

(10) For operational investments, OAs shall be performed until a decision is made to reevaluate the investment or to resume DME.

(11) All applicable decisions about system and service investments shall be reflected in new or updated entries (e.g., system, service, application) in the NRC information system inventory, as required by statute (44 U.S.C. Chapter 35, "Coordination of Federal Information Policy," among others) and OMB policy.

Responsibilities

Responsibilities of the Chairman

Review the IT budget request included in the overall agency budget recommended by the Executive Director for Operations (EDO) and the CFO and submit final recommendations to the Commission.

Responsibilities of the Commission

Review and approve the agency's IT budget request as part of the overall agency budget.

Responsibilities of the Executive Director for Operations

(1) Serve as the Chief Operating Officer and, as such, supervise the activities of the Assistant for Operations, who serves as the Performance Improvement Officer, in accordance with the GPRAMA.

(2) Ensure that the NRC's planning and budgeting process for IT investments is consistent and integrated with the agency's overall planning, budgeting, and performance management (PBPM) process.

(3) Ensure that program office and IT officials participate in the PBPM process for IT investments throughout their life-cycle.

(4) Ensure that statutory responsibilities for IT investments and their oversight are appropriately assigned to the agency's CIO.

(5) Together with the CFO, review and approve the selections and budget for the annual IT investment portfolio recommended by the IPEC and submit recommendations to the Chairman.

(6) Assign the CIO to be the Designated Approving Authority formally responsible for approving the operation of an IT system at an acceptable level of risk based on an agreed-on set of implemented security controls, in accordance with the Federal Information Security Management Act and NIST guidelines.

Responsibilities of the Chief Information Officer

Please refer to Appendix A, "Nuclear Regulatory Commission Chief Information Officer (CIO) Assignment Plan and Responsibilities."

(1) Assist and act for the EDO in executing the EDO's responsibility for IT infrastructure, application development, project management, information management services, and information system security oversight.

(2) Oversee, guide, and coordinate with the Deputy CIO and the Chief Information Security Officer.

(3) Develop and implement an agencywide framework of policies, processes, and procedures for IT investment management, strategic planning and EA, information and records management, and information security. This framework should support the NRC's mission, conform to Federal statutes and regulations and to OMB and GAO guidance, and be consistent with the NRC's overall PBPM programs.

(4) Co-chair the IPEC with the CFO, set the agenda for and facilitate meetings to achieve the IPEC's goals and objectives, and approve revisions to its charter, as needed.

(5) As a co-chair of the IPEC, jointly with the CFO, define the level of detail with which IT resources are described distinctly from other resources throughout the planning, programming, and budgeting stages. The level of detail provides transparency for the IT budget and serves as the primary input for the IT CPIC documents submitted to the OMB with the agency's overall budget.

(6) Review and approve the major IT portion of the budget request; the CFO shall affirm this CIO approval in the NRC's budget justification materials.

(7) Review and collaborate with program leadership on planned IT support for major program objectives and significant increases and decreases in IT resources.

(8) Jointly with the CFO, affirm that the IT portfolio contains appropriate estimates of all IT resources included in the IT budget request.

(9) Jointly with the CFO and the IPEC, provide an executive IT investment review function as required by the OMB, make decisions on the IT portfolio, and recommend the IT budget to the EDO for consideration in the NRC's overall budget.

(10) Establish other executive and technical review or advisory bodies, as necessary, to involve business and technical SMEs in IT investment planning and management oversight; ensure agencywide coordination; and fulfill CPIC requirements for IT investments, strategic planning and EA, security, and information and records management policies, as stated in the Capital Programming Guide and OMB Circular A-130.

(11) Jointly with the CFO and CAO, define agencywide policy for the level of detail of planned expenditure reporting for all transactions that include IT resources.

(12) As a member of the Strategic Sourcing Group, review and approve all acquisitions over $1 million, and provide oversight to ensure that all acquisition strategies and plans that involve IT apply adequate incremental development principles, use appropriate contract

types, contain appropriate statements of work for the IT portions, support the mission and business objectives in the IT strategic plan, and align with mission and program objectives (in consultation with program leadership).

(13) Review and approve all new IT purchases, regardless of dollar value.

(14) Recommend to the Commission any movement of funds for IT resources that requires congressional notification.

(15) Jointly with the CHCO, develop a set of competency requirements for IT and IT acquisition staff (including IT and IT acquisition leadership positions), and develop and maintain a current workforce planning process so 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 its mission. Continually assess the existing IT workforce to identify deficiencies and provide such assessments to the Chairman as part of the annual Human Capital Commission Briefing.

(16) Formally assume responsibility for operating major systems and networks at acceptable risk levels; evaluating the mission, business case, and budgetary needs for NRC systems in view of their security risks; and permitting or denying operations or use based on security risk.

(17) Provide an annual report on the NRC Cybersecurity Program, the NRC Privacy Program, and the findings of the NRC Inspector General's review of these programs, signed by the Chairman.

(18) Oversee the NRC Cybersecurity Program, which provides a quarterly report on the information security responsibilities of all senior agency officials, using a cybersecurity performance metric based on five major criteria: (1) computer security awareness training, (2) role-based training, (3) continuous monitoring, (4) cybersecurity incidents, and (5) phishing.

(19) As part of regular CIO evaluations, perform risk reviews covering three major areas: (1) managing active risks, (2) maintaining risk logs and actively managing risk mitigation strategies, and (3) identifying and managing risk triggers.

(20) As part of the CIO evaluations, review investments that meet the criteria for a TechStat. A TechStat is required for any high-risk investment that remains red or "at risk" for 3 consecutive months or more.

(21) Jointly with the CAO, share acquisition and procurement responsibilities. The CIO reviews all IT-related cost estimates and ensures that all acquisition strategies and plans that involve IT apply adequate incremental development principles.

Responsibilities of the Capital Planning and Investment Control Team

(1) Facilitate IT SME reviews for policy compliance, security, IT project management, and infrastructure impact, and consolidate SME recommendations for the IPEC.

(2) Facilitate IT investment reviews (e.g., Control Reviews, TechStats, CIO TouchPoints) with the CIO and appropriate IT governance boards.

(3) Coordinate with the Enterprise Architect to verify mapping between the NRC's EA and the Federal EA, and to ensure that investments align with the NRC's Strategic Plan, IT/IM Strategic Plan, and IT Roadmap.

(4) Coordinate with the NRC's Program and Project Management Team to establish project control gates and to ensure that project management standards and best practices are implemented throughout the life-cycle of each IT investment.

(5) Coordinate with other functional areas of OCIO on security-related requirements to support the development and review of IT business cases and project plans and the monitoring and evaluation of IT investments throughout their life-cycle.

(6) Help IT investment owners understand and comply with the CPIC process and related OMB requirements, including preparation of the NRC's IT Portfolio Summary and Major IT Business Case submissions.

(7) Work with IPTs and IT program and project managers for each major investment to update Major IT Business Cases and ensure complete and timely submission of updates to the OMB.

(8) Serve as a single point of contact for NRC inquiries about IT governance and CPIC processes and procedures.

(9) Coordinate input for the annual IT planning and budgeting guidance.

(10) Maintain an inventory of the agency's capitalized IT investments (i.e., Major IT Business Cases), and provide the current list to the Office of the Chief Financial Officer for inclusion in the NRC's budget justification materials.

(11) Provide input to educational outreach activities and training related to CCA, FITARA, and OMB requirements, and present training to IPTs and IT project managers on the CPIC portfolio and investment management and submission tool, OMB reporting requirements, and the NRC's IT governance.

(12) Establish requirements and criteria for selecting investments for the NRC's IT portfolio.

(13) Define and implement processes and procedures to monitor and evaluate IT investments throughout their life-cycle.

(14) Serve as the secretariat for the IPEC, scheduling meetings, developing agendas, coordinating briefings and reviews, taking minutes to document decisions and action items, and tracking action items to completion.

Other Responsibilities

Current charters fully describe and maintain the responsibilities of the IPEC, acquisition review boards, and IPTs. NRC Management Directive 2.8, "Integrated Information Technology/Information Management (IT/IM) Governance Framework," dated February 24, 2016, describes the responsibilities of the Enterprise Architect and the project management function. The NRC "Information Technology Asset Management Policy," issued in December 2016, describes the responsibilities of the hardware asset manager and software manager.

The NRC uses NUREG-1908, "Information Technology/Information Management Strategic Plan," to outline and refine internal processes, focusing on three key components: to empower, protect, and serve. Across both the public and the private sector, there is increased focus on using technology to create transparency and efficiency and to improve customer experience, both internally and externally. OCIO has completed a benchmark of the IT/IM Strategic Plan, and the NRC is in alignment with industry standards in both the private and the public sector.

As of November 2019, the NRC has met the requirements established by Congress in 2014, which include a special provision to the GAO to annually review agencies' data center inventories and strategies. The GAO's objectives were to (1) evaluate agencies' progress and plans for data center closures and cost savings, (2) assess agencies' progress against the OMB's data center optimization targets, and (3) identify effective agency practices for achieving data center closures, cost savings, and optimization targets. The GAO attained these objectives, presenting the results in GAO-16-323, "Data Center Optimization: Agencies Making Progress, but Planned Savings Goals Need to Be Established," dated March 4, 2016, and GAO-19-241, "Data Center Optimization: Additional Agency Actions Needed to Meet OMB Goals," dated April 11, 2019. The NRC has met all requirements for maintaining an inventory and consolidating and optimizing data centers, as posted in the OMB IT Dashboard.

Capital Planning and Investment Control Overview

The NRC CPIC is critical to the management and oversight of the agency's IT resources. It provides a mechanism for delivering high-quality information and recommendations to executive decision-makers on investments to be included in the IT portfolio.

Recognizing that IT investment management is dynamic, the NRC selects and continuously monitors and evaluates the investments in its IT portfolio to ensure that they effectively and efficiently support the agency's mission and strategic goals. The NRC's CPIC processes are designed to facilitate sound IT governance and the maturation of the NRC's IT investment management. The CPIC model relies on three distinct, yet interdependent, sets of processes: (1) Select, (2) Control, and (3) Evaluate. An investment can be active concurrently in multiple CPIC processes. After an investment is initially selected and funded, it repeatedly undergoes the Control and Evaluate processes for review and reselection until it is determined to have come to the end of its useful life, at which point it is decommissioned and removed from the IT portfolio.

Select

The purpose of the Select phase is to identify the IT investments, projects, and activities that best support the NRC's mission and current business needs at acceptable risk levels and as cost-effectively as possible. The key objectives are to analyze the risks and returns of each investment or project before committing funds, and to select or reselect those investments and projects that will best support mission needs.

The Select process and procedures capture IT investments and their supporting projects and resources for consideration in the overall IT portfolio. Investments considered include both new proposals and current investments being evaluated for reselection, either as-is or with enhancements. Investments being decommissioned also remain in the portfolio until they have been completely removed from the production environment and require no further funding. Investments are captured, categorized, analyzed, prioritized, and either selected, rejected, or placed on a lower priority or nonfunded list.

New IT investments proposed and selected for funding shall meet the following criteria:

- Gain approval from OCIO via the agency's Intake Technical Review Process, outlined here.
- Support the NRC's core or high priority mission functions.
- Fill a performance or capability gap in achieving the NRC's strategic goals and objectives, yielding the maximum benefits at the lowest life-cycle cost among viable alternatives.
- Support a function that no alternative private-sector or Government source can more efficiently support.
- Support work processes that have been simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial off-the-shelf technology.
- Demonstrate a projected best value, based on an analysis of quantifiable and qualitative benefits and costs and projected return on investment, that clearly equals or exceeds that of any alternative uses of available public resources.
  - Benefits contributing to best value may include improved mission performance in accordance with GPRA measures; reduced cost; increased quality, speed, or flexibility; and increased customer or employee satisfaction.
  - IT investment costs shall be adjusted for such risk factors as the investment's technical complexity, the organization's management capacity, the likelihood of cost overruns, and the consequences of under- or non-performance.
- Be consistent with applicable Federal and NRC enterprise and information architectures.
- Reduce risk by employing measures such as avoiding or isolating custom-designed components so that their failure would have minimal adverse effects on the overall project; using fully tested pilots, simulations, or prototype implementations before beginning production; establishing clear measures and accountability for project progress; and securing substantial stakeholder involvement and buy-in throughout the project.
- Be implemented in phased, successive segments, modules, sprints, or other useful units as narrow in scope and brief in duration as practicable, each solving a specific part of an overall mission problem and delivering a measurable net benefit independent of future segments or modules.
- Adhere to the standards in the NRC's Project Management Methodology 2.0, including the use of required artifacts.
- Adhere to security standards, including the use of required artifacts.
- Employ an acquisition strategy that allocates risk between the Government and contractors, effectively uses competition, ties contract payments to accomplishments, and takes maximum advantage of commercial technology.

Annually, the NRC shall review and evaluate all existing IT investments, based on data collected through the Control process and procedures and analyzed in the Evaluate process and procedures, to determine whether each investment meets the following criteria for reselection and funding:

- The investment continues to meet business needs and expected performance goals.
- Business needs and expected performance goals can be met more cost-effectively by maintaining, enhancing, or modifying the investment than by replacing it.
- The investment's current risk management plan and risk log show effective risk mitigation, including the management and closing of cybersecurity risks identified through continuous monitoring as listed on the investment's plan of actions and milestones.
- The investment adheres to projected costs and expected benefits throughout its life-cycle.

Control

The purpose of the Control phase is to ensure that, as projects develop and expenditures are made, each investment and its associated projects and activities continue to meet mission or business needs at the expected cost and risk levels. The key objectives are (1) to ensure quick corrective action to address any deficiencies in project or operational components, and (2) to enable the NRC to adjust investment objectives and modify expected outcomes if its mission or business needs have changed.

The Control process and procedures encompass various tools and techniques for monitoring and reporting on the performance of IT investments and the risks associated with them. These tools and techniques are key to obtaining high-quality data on the status of project costs and schedules, risks (including plans of actions and milestones), and investment performance, to inform decisions on changes to investments, projects, or the portfolio. The Control process and procedures include the annual updates and submissions of services, ledgers, and financial data; major IT investment monthly reviews and CIO evaluations; quarterly portfolio reviews; major IT investment control reviews; and CIO TouchPoints. Data and information collected from the monitoring of investments provide input for the evaluation of investments and support OMB reporting requirements.

Evaluate

The purpose of the Evaluate phase is to compare actual versus expected benefits and costs of IT investments and projects to assess return on investment, customer satisfaction, and value to the NRC in meeting its mission and business needs. The Evaluate phase has the following key objectives:

- Assess the capacity of a project or investment to meet performance expectations within cost and schedule limits and in compliance with IT policies.
- Identify any modifications needed on an investment (or on its associated projects or activities).
- Update IT investment management policies, processes, and procedures based on lessons learned.

The Evaluate process and procedures are used to analyze IT investment data to support the decision-making required to maximize the value of IT investments and the maturation of the IT portfolio and IT management practices. This entails performing annual OAs, PIRs, and TechStats, as needed. Although all of these activities inform the selection, reselection, and deselection of projects and investments within the IT portfolio, the OA is paramount. The NRC has based its OA

process on the requirements in Section III, “Management in Use,” of the Capital Programming Guide. The OA allows for a periodic, structured assessment of cost, performance, and risk trends over time to help determine when the cost and risk of an investment outweigh the value it provides.

Appendix A

Nuclear Regulatory Commission Chief Information Officer (CIO) Assignment Plan and Responsibilities

The following CIO Assignment Plan details decisions about certain IT resources included in the Common Baseline that the CIO delegates to other agency officials, as well as evidence that the CIO retains accountability in these areas. The CIO, through the Office of Chief Financial Officer, provides financial information to the Chairman and Commission. The CIO provides both the Chairman and the EDO the status of IT investments and the agency's IT Portfolio and activities on a regular basis. The CIO is responsible for the NRC IT Portfolio financial data. As OCIO receives inquiries from the Commission about the agency IT budget, CIO responds to this request. The CIO also participates in decision making meetings on the budget sent to the Chairman from the EDO.

"Assignment of Information Technology and Information Management (IT/IM) Responsibilities" delegating listed authorities to the CIO or equivalent lead official at the NRC.

FITARA section	Assignment Plan	Evidence that the CIO retains accountability
B CIO role in pre-budget submission for programs that include IT and overall portfolio	The CIO assigns responsibility for developing proposed IT planning, programming, and budgeting artifacts to the Division of Resource Management and Administration (DRMA), who coordinates with the Office of the Chief Financial Officer (OCFO), Program Offices, including CXOs. This group is comprised of budget, contract, acquisition, program management and HR. Each agency office ensures the accuracy of the information being reported, and after the CIO performs a final review.	The CIO approves IT planning, programming, and budget artifacts before they are submitted to OMB. The CIO approves artifacts based on Investment attestation of accuracy of reporting. OMB budget submissions will include information technology resource statementsthat affirm the CIO's review and approval of IT investmentsin the budget request, as well as changes to IT programs and resources.

FITARA section	Assignment Plan	Evidence that the CIO retains Accountability
C CIO role in planning program management	The CIO engages in program management through senior level management meetings including NRC Office Director meetings, Budget Formulation Process meetings, and Quarterly Program Review meetings.	The CIO approves planning and project management artifacts before they are submitted to OMB or implemented. The CIO approves artifacts based on Investment attestation of accuracy of reporting through OCIO and agencywide clearance processes. The CIO leads agency Annually, Quarterly and Monthly IT portfolio reviews as part of the CPIC Performance process.
D CIO reviews and approves the major IT investment portion of budget request	The CIO, with the support of Office Directors, approves the IT investments and budget request prior to the budget submission. The CIO assigns the responsibility for the accuracy of IT investments and financials information reported in the agency's budget request to each office, but always performs a final review.	The CIO approves planning, programming, and budget artifacts before they are submitted to OMB or implemented. The CIO approves artifacts based on office attestation of accuracy of all agency level Reporting for the Agency IT Portfolio.

FITARA section	Assignment Plan	Evidence that the CIO retains accountability
E Ongoing CIO engagement with program managers	The CIO assigns responsibilityfor Capital Planning and Investment Control (CPIC) performance reporting to the NRC IT investment Integrated Project Team (IPT). The CIO assigns responsibility for ensuring the accuracy of reported information as well as participating in regular portfolio and investment level reviews.	The CIO maintains accountability through the NRC IT governance structure and CPIC process. Additionally, the CIO maintains accountability through quarterly CIO evaluations which involve a review of risks, projects, costs, schedules, IT requirements, enterprise architecture and human capital.
F Visibility of IT planned expenditure reporting to CIO.	The CIO has visibility into the IT planned expenditures prior to the execution year. Every new or follow up acquisition is reviewed and approved by the CIO. Throughout the FY, the CIO reviews all execution year changes and must review any changes that occur across cost centers or BL PL Ps.	The CIO approves IT planned expenditure data. The data is reconciled in the NRC Agency Portfolio System, FEDPASS, and Capital Planning and Investment Control Performance Reporting. In regard to IT/IM Budget Guidance, the NRC has enhanced its budget execution process and procedures to better align budget formulation and budget execution, as well as provide improved visibility to all stakeholders. In FY 2020, OCFO implemented a new module within its Budget Formulation System (BFS) to capture the budget execution information. This new module, the Commitment Planning Module (CPM), is designed to track and document budget execution, and explain reallocations against formulated resources, while ensuring that appropriate plans are formulated prior to

		commitments. At the start of a fiscal year, Allowance Holders create Baseline contract/task order level commitment (execution) plans which align with the latest budget estimate. By aligning detail level contract plans against budgeted resources, CPM facilitates an early identification of resources for reallocation. With the additional goal of enhancing the CIO's visibility on budget execution, OCIO leveraged CPM to require CIO approvals for baseline commitment plans, as well as changes and reallocation requests on IT resources. The CIO approves reallocations throughout the year based on the OCIO reallocation approval guidance procedures. The agency has also implemented the consolidation of IT hardware and software purchases, as well as requiring offices to submit IT hardware and software purchases for enterprise architecture review.

G CIO defines IT processes and policies	The CIO assigns responsibility for defining development processes, milestones,review, and overall policies for project management and reporting for IT resources at the investment level to the Integration Program/Project Team. The IPTs then coordinate with their respective leadership and CXOs. These elements must remain in full compliance with NRC development processes, milestones, review gates, and overall policies for project management and reporting for IT resources as defined by the CIO.	The CIO issues agencywide guidance that defines development processes, milestones, review gates, and overall policies for project management and reporting for IT resources. Investments must fully comply with this guidance when developing investment level processes, milestones, review gates, and overall policies for project management and reporting for IT resources. OCIO posts agencywide IT policies and processes to the NRC intranet. https://www.nrc.gov/public-involve/open/digital-government/policyarchive/index.html

FITARA section	Assignment Plan	Evidence that the CIO retains accountability
H CIO role on program governance boards	The CIO and CFO co-chair the IPEC governance board and provide oversight for investment level IT governance bodies to voting members. Each NRC Office has a voting member and a back-up represented in the IPEC. IPEC is an executive management body established to determine U.S. Nuclear Regulatory Commission (NRC) Information Technology/Information Management (IT/IM) strategic direction and to manage its IT/IM portfolio by setting current fiscal year priorities and determining the funding of IT/IM investments that effectively integrate into the IT/IM portfolio, as required by the Clinger-Cohen Act, the Office of Management and Budget (OMB) Circular A-130, the Federal Information Security Management Act of 2002 (FISMA), and other Government requirements.	IPEC decides IT/IM direction, values, information security activities, and establishing the agency's risk tolerance for IT activities to achieve strategic program objectives; Approves major investments that will effectively integrate into the IT/IM Portfolio; Ensures the Agency's Capital Plan supports NRC's priorities; Reviews the IT/IM Portfolio in the year of execution to address current fiscal year priorities; Oversee the execution of the portfolio by reviewing the portfolio health on a quarterly basis against established direction, values and risk tolerance; and Communicates IPEC discussion and decisions to other NRC boards and/or committees. Each investment reports regularly to the CIO on its full IT governance structure and investment status.
I Shared acquisition and procurement responsibilities.	The CIO shares IT acquisition and procurement responsibilities with the office of Administration (ADM), which is responsible for the execution of all acquisition and procurements activities.	IT Budget Execution Guidance, MD 4.8, Budget Execution; NRC Acquisition of Supplies and Services, MD 11.1; Memorandum of Understanding Between Office of Administration, Office of the Chief Financial Officers and Regions, Capital Planning, and Investment Control Processes. The Office of the CIO and ADM have worked collaboratively to: define processes to ensure that the adequate use of incremental development is applied to IT acquisitions; develop formal procedures and training tutorials for the CORs and

		contractors to use in the execution and maintenance of various contracts or task orders; and the CIO is provided a report on a weekly basis that lists all requisitions received by the Acquisition team.
J CIO role in recommendin gmodification, termination or pause of IT	The CIO establishes thresholds for mandatory agency and investment level TechStat reviews as well as mandatory criteria for modification, termination, or pause of IT unless specifically exempted by the CIO. The CIO assigns investment level actions to CPIC and Enterprise Architecture, as well as the responsibility for auditing and ensuring the accuracy of all information reported to the agency for the CIO.	The CIO establishes thresholds for mandatory agency and investment level TechStat reviews as well as mandatory criteria for modification, termination, or pause of IT unless specifically by the CIO. TechStat Policy, Capital Planning, and Investment Control Processes as it is stated in the https://www.nrc.gov/public-involve/open/digital-government/policyarchive/index.html
K CIO review and approval of acquisition strategy and acquisition plan.	The CIO reviews and approves acquisition strategy and acquisition plan prior to contract award and ensures complete and accurate information in OMB Submission.	IT Budget Execution Guidance, MD 4.8, Budget Execution; NRC Acquisition of Supplies and Services, MD 11.1; Memorandum of Understanding Between Office of Administration, Office of the Chief Financial Officers and Regions, Strategic Sourcing Group Charter In response to the GAO request

		that the NRC provide supporting documentary evidence that acquisition office officials review acquisitions to ensure that IT is properly identified, NRC issued Acquisition Instruction (AI) #2018-01, Identifying IT Related Acquisitions, on June 25, 2018. As this AI has been shared with NRC program offices and regions, NRC is fully compliant with FITARA Section K- Acquisition.