Capital Planning and Investment Control Policy and Overview

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

Version 2.0

October 2016

Revision History

Date	Version	Summary of Changes	Author
09/28/2015	1.0	Updated IT CPIC policy to reflect FITARA and associated OMB requirements. Under FITARA, this policy is now publicly available. 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 on 11/01/2015. ADAMS Accession No. ML15288A545.	Vickie Smith, OCIO/PMPD/IPMB Approved by Darren Ash, CIO
10/21/2016	2.0	Significant updates were made to reflect new policy requirements in the revised OMB Circular A-130, "Managing Information as a Strategic Resource" (July 2016); OMB Memorandum, "Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reuseable and Open Source Software" (M-16-21); and OMB Category Management Policy for Common IT. ADAMS Accession No. ML16272A383	Vickie Smith, OCIO/PMPD/IPMB Approved by David Nelson, CIO

Note: The NRC maintains detailed processes and operating procedures in separate documents to support continuous refinement of the NRC's maturing investment management. This document sets forth CPIC Policy and provides an overview of CPIC processes.

Table of Contents

Background and Authorities

Capital Planning and Investment Control (CPIC) for information technology (IT) investments refers to "a decisionmaking 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 (CCA) of 1996 (Public Law 104-106, formerly known as the IT Management Reform Act of 1996), requires Federal agencies to use a disciplined CPIC process to acquire, use, maintain, and dispose of IT assets. While other laws (e.g., the Paperwork Reduction Act of 1980 and 1995, Government Performance and Results Act of 1993 (GPRA), GPRA Modernization Act of 2010 (GPRAMA), Federal Acquisition Streamlining Act of 1994) also required agencies to develop and implement a disciplined process to maximize the value of IT investments while balancing risks, 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, CCA mandates that agencies implement CPIC processes that shall:

(1) Provide for the selection, control, and evaluation of agency IT investments.

(2) Be integrated with the processes for budget, financial, and programmatic decision-making.

(3) Include minimum criteria for considering whether to undertake an IT investment.

(4) Identify IT investments that would result in shared benefits or costs for other Federal agencies or State or local governments.

(5) Provide the means for identifying quantifiable measurements for IT investment net benefits and risks.

(6) Provide the means for senior management to obtain timely information regarding an investment's progress.

More recently, additional requirements have been established by the Federal Information Technology Acquisition Reform Act (FITARA), enacted on December 19, 2014. The Office of Management and Budget (OMB) issued guidance on implementing FITARA in OMB Memorandum, "Management and Oversight of Federal Information Technology," (M-15-14) on June 10, 2015. FITARA builds upon CCA by empowering Federal Chief Information Officers (CIOs) with increased oversight over the following: (1) budget planning, (2) governance structures, (3) portfolio risk management, (4) hiring practices within the IT offices, (5) data center consolidation planning and execution, and (6) reporting progress and metrics to OMB. To build upon and strengthen the CPIC requirements of CCA, FITARA establishes the Common

[1] Definition provided by the Office of Management and Budget in the Integrated Data Collection Common Definitions. See 40 U.S.C. 11302 for statutory requirements and the Clinger-Cohen Act of 1996.

Baseline for IT Management, defining the roles and responsibilities of the CIO and other senior agency officials while ensuring the CIO retains accountability.

To further assist agencies with meeting the requirements set forth in CCA and FITARA, OMB issues the annual *IT Budget and Capital Planning Guidance* as part of OMB Circular A-11, "Preparation, Submission, and Execution of the Budget," (Circular A-11) and maintains its supplement, the *Capital Programming Guide,* to assist agencies with the implementation of CPIC processes and meeting reporting requirements to Congress. OMB Circular A-130, "Managing Information as a Strategic Resource," (Circular A-130) as revised July 2016, provides additional guidance for implementing CPIC and FITARA requirements. OMB updates these circulars based on current, relevant statues and Executive Orders.

As part of FITARA, OMB has also issued Category Management Policy in a series of memoranda, including the following:

- OMB Memorandum, "Category Management Policy 15-1: Improving the Acquisition and Management of Common Technology: Laptops and Desktops," issued October 16, 2015
- OMB Memorandum, "Category Management Policy 16-1: Improving the Acquisition and Management of Common Technology: Software Licensing," issued June 2, 2016
- OMB Memorandum, "Category Management Policy 16-3: Improving the Acquisition and Management of Common Technology: Mobile Devices and Services," issued August 4, 2016

On August 8, 2016, OMB also issued OMB Memorandum, "Federal Source Policy: Achieving Efficiency, Transparency, and Innovation" (M-16-21). 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 CPIC policy for the NRC. 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, Circular A-130, OMB Category Management Policy, and M-16-21 requirements; therefore, it supersedes all previous version of the NRC's CPIC policy. This document also provides a brief overview of the NRC CPIC processes. It is worth noting that CPIC processes and procedures are continuously evaluated and refined; therefore, detailed processes and procedures are maintained in separate documents. This allows for timely updates and implementation and is consistent with best practices. It also supports the NRC's goal to continuously mature its IT investment management practices to achieve an IT portfolio that leverages IT for strategic outcomes in support of the NRC's mission.

Definitions

Definitions provided in this section help lay the foundation for, and build better understanding of, the CPIC policy and processes.

Adequate Incremental Development refers to the planned and actual delivery of new or modified technical functionality to users at least every six months during the development of software or services.

Agile Software Development refers to a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen tight iterations throughout the development cycle. Managing agile software development projects is fundamentally no different than managing any project. You still must deal with the "iron triangle" (Cost, Schedule, Scope) but there are many very small iron triangles. At a macro level the project manager still must estimate, monitor, and control these three elements to ensure project success.

Alternative Analysis refers to a method for addressing the various options for meeting the performance objectives of an investment, including the estimated return on investment (ROI), and if applicable, estimated cost savings or cost avoidance, of the various options. The analysis is performed prior to the initial decision to implement a solution and updated periodically, as appropriate, to capture changes in the context for an investment decision. This terms refers to best practices outlined in the *Capital Programming Guide* under Section I.4, “Alternatives to Capital Assets" and Section 1.5, "Choosing the Best Capital Asset.”

Note: Alternatives Analysis shall be performed for investments with projects in the planning or DME stages, whereas strictly operational investments shall instead perform operational analyses until such time as a decision is made to re-evaluate the investment or to resume development, modernization or enhancement.

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

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

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 investments to achieve the agency’s strategic goals and objectives with the lowest overall cost and least risk.

CIO Evaluations refers to the CIO's best judgment of the current level of risk for an investment in terms of its ability to accomplish its goals (40 USC 11315(c)(2)). The evaluation should be informed by the following factors, including, but not limited to: (1) risk management; (2) requirements management; (3) contractor oversight; (4) historical performance: (5) human capital; (6) and other factors that the CIO deems important to the forecasting future success. Each evaluation includes a narrative to explain the rating; this is particularly important whenever the rating has changed since the last evaluation.

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 and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud). Key enabling technologies include: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware.

Cloud First Policy refers to OMB's Cloud First policy, launched in December 2010, which is intended to accelerate the pace at which the government realizes the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.

Note: Per the Federal Cloud Computing Strategy, agencies shall:

- *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 in order 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 lifecycle stage.*

Commodity IT refers a category of back-office IT services whose functionality applies to most, if not all, agencies (e.g., infrastructure and asset management, email, hardware and software acquisition, and help desks). This also relates to OMB's PortfolioStat initiative and a CIO-lead business approach to the delivery of IT infrastructure, enterprise IT, and administrative/business systems that emphasizes pooling agencies' purchasing power across their entire organization through shared services as a provider or consumer, instead of standing up separate independent services to eliminate duplication, rationalize the agency's IT investments, and drive down costs.

There are three categories of Commodity IT:

- Enterprise IT – Items that pertain to this are: Email; Collaboration; Identity and Access Management; IT Security (Not Identity and Access Mgmt.); and Web Hosting, Infrastructure, and Content

- IT Infrastructure - Items that pertain to this are: Desktop Systems; Mobile Devices; Mainframes and Servers; and Telecommunications

- Business Systems - Items that pertain to this are: Financial Management; Human Resources Management; Grants-Related Federal Financial Assistance; Grants-Related Transfer to State and Local

Cost is defined in *Statement of Federal Financial Accounting Concepts (SFFAC) No. 1, Objectives of Federal Financial Reporting*, as the monetary value of resources used. Defined more specifically in *Statement of Federal Financial Accounting Standards (SFFAS) No. 4, Managerial Cost Accounting Concepts and Standards for the Federal Government*, 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 nature of the transaction, cost may be charged to operations immediately (i.e., recognized as an expense of the period) or 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*, "cost" is used synonymously with expense.

Cost Avoidance is an action taken in the immediate timeframe that will decrease costs in the future. For example, an engineering improvement that increases the mean time between failures and thereby decreases operation and maintenance costs is a cost avoidance action, as defined in OMB Circular A-131, “Value Engineering” (Circular A-131).

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

Development, Modernization, and Enhancement (DME) refers to projects and activities leading to new IT assets or systems, as well as projects and activities that change or modify existing IT assets to substantively improve capability or performance, implement legislative or regulatory requirements, or meet an agency leadership request. DME activity may occur at any time during a program’s lifecycle. As part of DME, capital costs can include hardware, software development and acquisition costs, commercial off-the-shelf acquisition costs, government labor costs, and contracted labor costs 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 completed or a replacement asset has superseded it; disposition costs may be included in operational activities near the end of the useful life of an asset.

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/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. The qualities and operating characteristics of earned value management systems (EVMS) are described in American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard–748–1998, "Earned Value Management Systems."

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

Enterprise Architecture (EA) refers to the strategic business, technology and documentation of the current and desired relationships among business and management processes and IT of an organization. An EA includes the rules and standards and systems lifecycle information to optimize and maintain the environment which the agency wishes to create and maintain through its IT portfolio. An EA must provide a strategy that enables the agency to support its current state and provides a roadmap for transition to its target environment. An EA defines principles and goals and sets a direction on such issues as the promotion of interoperability, open systems, publics access, end-user satisfaction, and IT security.

Note: While 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 roadmap provides current views, future views, and transition plans at an appropriate level of detail for all IT investments, services, systems, and programs. It should also contains an IT asset inventory using the FEA Reference Models and other attachments or appendices for CPIC, EA, shared service, and other planning products requested by OMB that provide additional information regarding roadmap plans.

Federal IT Dashboard (ITDB) refers to a website (www.itdashboard.gov) that enables Federal agencies, industry, the general public, and other stakeholders to view details regarding the performance of Federal IT investments. The ITDB is used by the Administration and Congress to inform budget and policy decisions.

Financial Management Systems refers to systems necessary to support financial management, including automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. The following are examples of financial management systems: (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. See OMB Circular A-127, "Financial Management Systems" (Circular A-127), for additional information and guidance.

Functional/Business Sponsor refers to the agency official who is responsible for the program or function supported or implemented by the investment (44 U.S.C. 3501 (a) (4)). The sponsor is responsible for expressing the value of, ensuring successful implementation of, and providing

accurate and timely data for the IT investment to the agency CIO and OMB. The designated person may (or may not) be the same as the "Business Process owner/Subject Matter Expert" serving on the Integrated Program Team (IPT). Each major and non-major IT investment must include the name of the functional/business sponsor as well as the individual's title,

Information Resources Management (IRM) Strategic Plan refers to a document that addresses all information resources management of an agency. 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's strategic plan that is required in OMB Circular A-11; provide a description of how information resources management activities help accomplish the agency's missions delivery area and program decisions; and ensure 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, disruptions, modification, or destruction, as well as the creation and implementation of security policies, procedures and controls. It includes the development, implementation, and maintenance of security policies, procedures, and controls across the entire information lifecycle. These functions should include implementation and activities associated with National Institute of Standards and Technology (NIST) 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," including (1) security awareness training (but not the technical infrastructure required for the delivery of training); (2) FISMA compliance reporting; (3) development of a security policy; and (4) security audits and testing.

Note:

- *IT security should include systems that oversee Agency IT needs.*
- *Do Not Include IT costs related to Identity or Access Management systems/solutions.*
- *Do Not Include physical protection of an organization (e.g., guards, cameras, and facility protection).*

Information System refers 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 is defined as:

A. Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where

B. such services or equipment are 'used by an agency' if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

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

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

IT Asset refers to anything (tangible or intangible) that has value to an organization, including, but not limited to: a computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards) as well as 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 / investment and tracked and monitored throughout its lifecycle in accordance with the NRC's IT Asset Management (ITAM) processes.

IT Investment refers to the expenditure of IT resources to address mission delivery and management support. An IT investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or group of IT assets with related functionality, and the subsequent operation of those assets in a production environment.

Note: All IT investments shall have a defined lifecycle with start and end dates, with the end date representing the end of the currently estimated useful life of the investment, consistent with the investment's most current alternatives analysis if applicable. When the asset(s) is essentially replaced by a new system or technology, the replacement shall be reported as a new, distinct investment, with its own defined lifecycle information.

There are four types of IT investments:

- **Funding Transfer Investment** refers to the portion of funding a partner agency provides funding contributions to another IT investment. The description of the IT investment should indicate the Unique Investment Identifier (UII) of the managing partner investment.

  Note: The NRC is a partner agency of multiple funding transfer investments (i.e., E-Govs, Lines of Business (LoBs), and shared services) and therefore shall budget for, and report the funding provided to the agency managing the investment, on its IT Portfolio Summary submitted to OMB. During the selection process, funding transfer investments shall be included as an alternative considered in the alternative analysis. If not selected, a business justification for the solution selected must be approved by the CIO and submitted to OMB for approval.

- **IT Migration Investment** refers to the portion of a larger asset to track the migration costs associated with systems in the partner agency that are not captured either by the managing partner or the interfacing systems. The description of the IT investment should indicate the UII of the major IT investment of the managing partner the partner agency is migrating to.

  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 do so under an IT migration investment on its IT Portfolio Summary. When migrating to a new investment that is not a funding transfer investment, the cost will be reported as planning DME on the new investment's lifecycle cost table.

- **Major IT Investment** refers to an IT investment requiring special management attention because of its importance to the mission or function to the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; unusual funding mechanism; or definition as major by the agency's CPIC process. This includes all "major automated information system" as defined in 10 U.S.C. 2445 and all "major acquisitions" consisting of information resources as defined in the *Capital Programming Guide*. 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 regarding which investments are considered "major."

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

IT Program Managers (IT PgMs) and IT Project Managers (IT PMs) refers to the Integrated Program/Project Team (IPT) members responsible for IT investments and lead the required IPT for the investment. In some cases, IT PgMs and IT PMs can hold positions in other classification series; however they must still meet the requisite Federal certification and/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 includes all:

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

B. Acquisitions or interagency agreements that include IT and the services or equipment provided by such acquisitions or interagency agreements; but

C. Does not include grants to third parties which establish or support IT not operated directly by the Federal Government.

IT Service refers to a means of delivering IT, in combination with any inherent people or processes, of value to customers by facilitated outcomes customers want to achieve without the ownership of specific costs and risks.

Integrated Program/Project Team (IPT) is defined as a multi-disciplinary team led by an IT PgM/PM responsible and accountable for planning, budgeting, and procurement and lifecycle management of the investment to achieve its cost, schedule, and performance goals. Team skills include: budgetary, financial, capital planning, procurement, user, program, architecture, EVM, security, and other staff as appropriate.

Note: In order for OMB to approve the budget for a major IT investment, its IPT must include at a minimum:

- *a qualified, fully dedicated IT program manager*
- *a contracting specialist, if applicable*
- *an IT specialist*
- *an IT security specialist*
- *a business process owner or subject matter expert (SME).*

Other members of the IPT might include:

- *enterprise architects*
- *IT specialists with specific expertise in data, systems, or networks*
- *capital planners*
- *performance specialists.*

Key members of the IPT should be co-located during the most critical junctures of the program, to the maximum extent possible. Agencies should establish IPT members' individual performance goals to hold team members accountable for both individual functional goals and the overall success of the program. The investment IPT should be defined in a program or an IPT Charter.

Interagency Acquisition refers to the use of the Federal Supply Schedules; a Multi-Agency 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 OMB pursuant to Section 11302(3) of the Clinger-Cohen Act of 1996).

Lifecycle Costs refers to all investment costs, including government Full Time Equivalents (FTE), from the commencement of the investment through its estimated useful life (or the composite estimated useful life of the assets within the investment), independent of the funding source (e.g.,

revolving fund, appropriated fund, working capital fund, trust fund). For more information about lifecycle costs, see the *Capital Programming Guide* and Circular A-131.

Maintenance refers to the activity necessary to keep an asset functioning as designed during the operations and maintenance (O&M) phase of an investment. Maintenance activities may also include, but are not limited to, operating system upgrades, technology refreshes, and security patch implementations. As defined in the *Federal Accounting Standards Advisory Board Statement of Federal Financial Accounting Standards Number 10*, maintenance excludes activities aimed at expanding the capacity of an asset 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 and/or duration with pre-determined start and end dates should be managed as projects and reported on the project and activities tables in Section B of Major IT investment Update.

Managing Partner refers to the lead agency that is responsible for coordinating the implementation of the funding transfer investments. The managing partner maintains an IT shared service with approval by agency leadership for intra-agency services, and also by OMB for inter-agency services. The managing partner organization, often referred to as the Program Management Office (PMO), develops, implements, and maintains financial and service models as well as contracts with customers and suppliers using strategic sourcing vehicles whenever practicable. The managing partner PMO is responsible for the success of the IT shared service, and reports using metrics developed by the Federal Agency for its own intra-agency IT shared services, and by the Federal CIO Council's Shared Services Subcommittee for inter-agency LOBs. 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 breaking down an investment into one or more projects, increments or useful segments, each of which produces a measurable result towards delivering the functionality or capability identified in the investment's business case. Projects produce a useable system or functionality that can be implemented and used effectively independent of future projects.

Operational Analysis refers to a method of examining the ongoing performance of an operating asset investment and measuring that performance against an established set of cost, schedule, and performance goals. An operational analysis is, by nature, less structured than performance reporting methods applied to developmental projects and should trigger considerations of how the investment's objectives could be better met, how costs could be reduced, and whether the organization should continue performing a particular function. Guidance for Operational Analysis is described in the *Capital Programming Guide*. Best Practices can also be found in the Government Accountability Office report, "Information Technology: Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments" (GAO-13-87).

Operations refers to the day-to-day management of an asset in which the asset is in the operations production environment and produces the same product or provides a repetitive service. Operations include, but are not limited to, activities that operate data centers, help desks, operational centers, telecommunication centers, and end-user support services.

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

Partner (Customer) Agency refers to the agency in an inter/intra agency collaboration, such as an E-Gov, LoB initiative or Federal shared service, that contracts with and pays a managing partner to receive an IT shared service. The customer agency organization may be required to interact with a supplier for the coordination of day-to-day service issues. The managing partner handles major contract issues and resolves escalation items with suppliers. 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, and reflecting the amount of the contribution for each of the initiatives to which the agency provides resources.

Planning refers to preparing, developing, or acquiring the information used to design the asset; assess the benefits, risks, and risk-adjusted costs of alternative solutions; and establish realistic cost, schedule, and performance goals for the selected alternative, before either proceeding to full acquisition of the capital project or useful component or terminating the project.

Note: Planning must progress to the point where the agency is ready to commit to achieving specific goals for the completion of the acquisition before proceeding to the acquisition phase. Information gathering activities to support planning may include:

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

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

Post-Implementation Review (PIR) refers to an evaluation of how successfully the investment or project objectives were met and how effective the project management practices were in keeping the investment or project on track. A PIR can be conducted after a project has been completed, or

after an investment concludes the implementation phase. Additional details regarding the PIR process is described in the *Capital Programming Guide*.

Privacy Impact Assessment (PIA) refers to the process for examining the risks and ramifications of using IT to collect, maintain, and disseminate information from or about members of the public in an identifiable form. The process is also used to identify and evaluate protections and alternative processes to mitigate the impact to privacy of collecting such information. Consistent with OMB guidance regarding implementing the privacy provisions of the E-Government Act (M-03-22), agencies must conduct and make publicly available PIAs for all new or significantly altered IT investments that administer information in an 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 a temporary endeavor undertaken to accomplish a unique product or service with a defined start and end point and specific objectives that, when attained, signify completion. Projects can be undertaken for the development, modernization, enhancement, 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 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 to overall objectives. Risk management should be conducted throughout the entire lifecycle of the program.

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

Shadow (Hidden) IT refers to spending on IT that is not fully transparent to the Agency CIO and/or IT resources included as a portion of a program that is not primarily of an "information technology" purpose but delivers IT capabilities or contains IT resources. For example, a grants program that contains a portion of its spending on equipment, systems, or services that provide IT capabilities for administering or delivering the grants. If the CIO is not aware of and involved in the programming, it is considered shadow IT.

Shared Service refers to a service that is provided by one Federal organization to other Federal organizations that are outside of the provider's organizational boundaries. Shared services may

be intra-agency or inter-agency. There are three categories of shared services in the Federal Government:

- **Mission Services** - core purpose and functional capabilities of the Federal Government, such as disaster response, food safety, national defense, and employment services.
- **Commodity IT** – including IT infrastructure and Enterprise IT services
- **Support Services** –capabilities that support common business functions performed by nearly all Federal organizations, such as budgeting, financial, human resources, asset, and property and acquisition management.

Note: Shared Commodity IT and Support Services are considered to be IT; associated costs must be included/reported as part of the IT Portfolio Summary.

Shared Service Provider refers to the provider of a technical solution and/or service that supports the business of multiple agencies using a shared architecture. For multi-agency services, this is the managing partner of the investment.
Unique Investment Identifier (UII) refers to a persistent numeric code applied to an investment that allows the identification and tracking of an investment across multiple fiscal years (FYs) of an agency's IT portfolio. The UII is composed of a three-digit agency code concatenated with a nine-digit unique investment number generated by the agency. Some nine-digit numbers are reserved for OMB to assign to funding transfer investments and may not be assigned by agencies.

CPIC 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 unless stated as applying to only 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 OMB during the annual budget submissions.

2. For major IT investments, a Major IT Business Case must also be developed and maintained for justifying the budget request to, and reporting performance and the expenditure of IT resources to, 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 greater than or equal to 10 percent of the agency IT budget [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 Circular A-127
- defined as major by the NRC CPIC process

All other IT investments are considered non-major IT investments with the exception of funding transfer investments and IT migration investments used by the NRC. The NRC is a partnering agency to a number of investment 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 on 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 executive investment review board (IRB). Budgeting for IT resources in all programs (not just programs that are primarily IT-oriented) shall be done in accordance with the IT Budget Guidance issued by the Office of the Chief Information Officer (OCIO) and in tandem with the overall agency budget formulation process issued by the Office of the Chief Financial Officer (OCFO).

5. As a chair of the executive IRB, the CIO shall advise on and approve the IT aspects of all programs. In the case of major IT investments, additional, more extensive involvement shall occur through the monthly updates, CIO evaluations, and CIO TouchPoints.

6. The IT budget formulation process and annual Agency IT Portfolio Summary and Major IT Business Case submission process shall ensure that the budget justification materials, in their initial budget submission, receive the appropriate CIO approvals and certifications, and include affirmation statements of these approvals and certifications, as listed and described in Circular A-130 and Circular A-11.

7. The CIO and Chief Financial Officer (CFO) shall define, and as the co-chairs of the executive IRB, provide oversight of, the process by which the CIO, CFO, Chief Acquisition Officer (CAO), and Chief Human Capital officer (CHCO) information technology shall work with program leadership to plan an overall IT portfolio that efficiently and effectively leverages IT for strategic outcomes in support of the NRC's program and business objectives aligned to Agency Strategic Plan. This includes defining the level of detail at which IT resources are budgeted and in consultation with the CAO, defining processes to track planned expenditures for IT resources against actual expenditures for all transactions that include IT resources.

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

8. An IT investment's justification, cost, schedule, measurement indicators, and other management and technical artifacts shall describe its discrete and unique set of IT products and services and how they support the NRC mission or mission support functions. All major IT investments shall document and report all of the above through the formal Major IT Business Case and Required Artifact Submissions to OMB[3].

9. Major IT investments shall adhere to *Principles of Budgeting for Capital Asset Acquisitions* set forth by OMB in Appendix 6 of the *Capital Programming Guide*.

10. Two or more IT investments shall not deliver the same discrete and unique set of IT products or services and shall not serve the same purpose. If duplicative investments are identified, an alternative analysis shall be performed and a plan developed to eliminate the duplication and associated cost.

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

12. All IT investments shall have a defined lifecycle with start and end dates, with the end date representing the end of the currently estimated useful life of the investment, consistent with the investment's most current alternatives analysis if applicable. When the asset(s) is essentially replaced by a new system or technology, the replacement shall be reported as a new, distinct investment, with its own defined lifecycle 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 lifecycle.

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

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

16. When conducting an alternative analysis for a new investment, the Three-Step Software Solutions Analysis, as described in M-16-21 Federal Source Code Policy shall be performed.

[3] NRC CPIC procedures for Major IT Business Cases are based on annual fiscal year IT Budget and Capital Planning Guidance issued as part of OMB Circular A-11.

17. In the case of a new major IT investment, a full business case must be developed. Once approved by the CIO, the initial business case will serve as the basis for the Major IT Business Case submitted to the ITDB. The business case will then be maintained through the Major IT Business Case and Major IT Update submission processes.

18. 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 to strengthen the understanding of requirements.

19. All acquisition planning shall adhere to the planning provisions set forth in FAR Subpart 7.1, “Acquisition Plans,” and Part 10, “Market Research.”

20. Planning for IT acquisitions shall substantiate the NRC’s commitment to achieve specific goals for the completion of the acquisition. Planning activities and results shall be documented and final plans approved before proceeding to the acquisition phase. For investments developed or managed using an iterative or agile methodology, ensure proper planning for each iteration or sprint is conducted throughout the entire acquisition.

21. All IT hardware and software will be planned, acquired, deployed, managed, and disposed of under an IT investment on the NRC’s IT Portfolio Summary and in accordance with the NRC’s IT Asset Lifecycle Management processes and procedures.

22. When 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 consider factors, such as, but not limited to:
    - alignment to the NRC’s Strategic Plan
    - the ability to meet operational or mission requirements
    - conformance to the current and target EA and alignment to the Enterprise Roadmap
    - total lifecycle cost of ownership and the ability to sustain such costs
    - performance
    - security risks
    - interoperability
    - privacy
    - accessibility
    - ability to share or reuse
    - resources required to switch vendors to avoid “being locked in”
    - availability of quality support at a reasonable cost

23. Decisions to improve, enhance, or modernize existing IT investments or to develop new IT investments will be made only after conducting an alternatives analysis that includes both government-provided (internal, interagency, and intra-agency where applicable) and commercially available options, and the option representing the best value to the Government has been selected.

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

25. Decisions to acquire custom or duplicative solutions must be justified based on overall lifecycle cost-effectiveness or ability to meet specific and high-priority mission or operational requirements.

26. 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 such information consistent with NIST standards and guidelines.

Acquiring Information Technology and Services

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

- 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:
  - Laptops and Desktops (M-16-2)
  - Software Licensing (M-16-12)
  - Mobile Devices and Services (M-16-20)
- the FAR, including the planning provisions set forth in FAR Subpart 7.1, “Acquisition Plans,” and Part 10, “Market Research” prior to an acquisition
- NRC Management Directive (MD) 11.1, “NRC Acquisition of Supplies and Services”

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

1. Develop a thorough Cost Benefit Analysis of all procurement requirements based upon market research which includes an Alternative Analysis.

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

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

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

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

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

7. To the extent practicable, modular contracts for IT, including orders for increments or useful segments of work, should be awarded within 180 days after the solicitation is issued. If award cannot be made within 180 days, agencies shall consider cancelling the solicitation. The IT acquired should be delivered within 18 months after the solicitation resulting in award of the contract was issued.

8. Align IT procurement requirements with the Agency's strategic goals.

9. Promote innovation in IT procurements, including conducting market research in order to maximize utilization of innovative ideas.

10. Include security, privacy, accessibility, records management, and other relevant requirements in solicitations.

11. Ensure that all acquisition strategies, plans, and requirements (as described in FAR Part 7), or interagency agreements (such as those used to support purchases through another agency) that include IT are reviewed and approved by the CIO. 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 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 Government-wide IT requirements, such as information security.
    - Opportunities to migrate from end-of-life software and systems, and to retire those systems.

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

13. All acquired IT hardware and software will be entered into the NRC's IT asset inventory and management tool(s).

IT Investment Design and Management

The NRC shall, to extent practical 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. Information systems, technologies, and processes shall facilitate accessibility under the Rehabilitation Act of 1973, as amended; in particular, see specific electronic and IT accessibility requirements, commonly known as Section 508 requirements.
4. Records management functions and retention and disposition requirements must be fully incorporated into information lifecycle processes and stages, including the design, development, implementation, and decommissioning of information systems, particularly Internet resources to include storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service.
5. A PIA and Security Impact Assessment must be performed upfront and the appropriate security planned, budgeted, and built-in at the start of the project.
6. IT investments use an Earned Value Management System (EVMS) and Integrated Baseline Review, when appropriate, as required by FAR Subpart 34.2. When an EVMS is required, agencies must have a documented process for accepting a contractor's EVMS. When an EVMS is not required, implement a baseline validation process as part of an overall investment risk management strategy consistent with OMB guidance.
7. All IT development projects shall appropriately implement incremental development and modular approaches as defined in OMB guidance titled, "Contracting Guidance to Support Modular Development," issued June 14, 2012.
8. Maintenance activities of notable cost and/or duration with pre-determined start and end dates should be managed as projects. In the case of major IT investments, project and activities tables in Section B of Major IT investment Update shall be used to track, monitor, and report the cost and schedule.
9. For operational investments, an operational analyses shall be perform until such time as a decision is made to re-evaluate the investment or to resume development, modernization or enhancement.

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 Chief Financial Officer (CFO) and submit final recommendations to the Commission.

Responsibilities of the Commission

Review and approve the agency's IT budget request included in the overall agency budget.

Responsibilities of the EDO

1. Serve as the Chief Operating Officer (COO) 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 lifecycle.
4. Ensure that statutory responsibilities regarding IT investments and their oversight are appropriately assigned to the agency CIO.
5. Together with the CFO, review and approve the selections and budget for the annual IT investment portfolio recommended by the executive level IT investment review board and submit recommendations to the Chairman.
6. Assign the Deputy Executive Director for Reactor and Preparedness Programs (DEDR); the Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration, and Human Capital (DEDM); and the CIO to be the Designated Approving Authority (DAA) to assume formal responsibility for approving the operation of an IT system at an acceptable level of risk based on an agreed-upon set of implemented security controls, in accordance with FISMA and guidelines set forth by the NIST.

Responsibilities of the CIO

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 systems security oversight.
2. As the CIO, carry out the supervision, guidance, and coordination of the Deputy Director, Office of the Chief Information Officer (OCIO) who serves as the Deputy Chief Information Officer (DCIO) and of the Chief Information Security Officer (CISO).

3. Develop and implement an agencywide framework that includes policies, processes, and procedures for IT investment management, strategic planning and enterprise architecture, information and records management, and information security that supports NRC's mission, meets the requirements of Federal statutes and regulations, and guidance from OMB and the GAO, and is consistent with the NRC's overall planning, budgeting, and performance management programs.

4. Co-chair the executive level IRB with the CFO, set the agenda for and facilitate meetings to meet the IRB's goals and objectives, and approve revisions to its charter, as needed.

5. As co-chair of the executive level IRB, 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 shall provide transparency into the IT budget and serve as the primary input into the IT CPIC documents submitted to OMB with the agency budget.

6. Review and approve the major IT portion of the budget request; the CFO shall provide affirmation of 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 includes appropriate estimates of all IT resources included in the IT budget request.

9. Jointly with the CFO and executive level IRB, provide an executive IT investment review function as required by 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 comply with CPIC requirements for IT investments, strategic planning and enterprise architecture, security, and information and records management policies, as stated in the *Capital Programming Guide* and 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 acquisitions to ensure all acquisition strategies and plans that include 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 supported by the IT strategic plan, and align mission and program objectives in consultation with program leadership.

13. Review and approve all new IT purchases regardless of dollar threshold.

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 to ensure the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the IT talent needed to accomplish the mission.

16. Jointly with the DEDR and DEDM, formally assume the responsibility for operating a major system or network at an acceptable level of risk; evaluating the mission, business case, and budgetary needs for an NRC system in view of the security risks; and permitting or denying operations or use based on unacceptable security risk.

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 the SME recommendations for executive level and management level IRBs.

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

3. Coordinate with the NRC's EA 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 enterprise roadmap.

4. Coordinate with NRC's Project Management Branch (PMB) to establish project control gates and to ensure project management standards and best practices are implemented throughout the IT investment lifecycle.

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 lifecycle.

6. Assist IT investment owners in their understanding and compliance 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 PgMs/PMs for each major investment to update Major IT Business Cases and ensure complete and timely submission of updates to OMB.

8. Serve as a single point-of-contact for NRC inquiries regarding IT governance and CPIC processes and procedures.

9. Coordinate input to 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 OCFO 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 related to CPIC's portfolio and investment

management and submission tool, OMB reporting requirements, and the NRC's IT governance to IPTs and all PMs.

12. Establish requirements and criteria for the selection of IT investments comprising the NRC's IT portfolio.

13. Define and implement processes and procedures to monitor and evaluate IT investments throughout their lifecycle.

14. Provide a secretariat function for the executive level and management level IT investment review boards, including scheduling meetings, developing agendas, coordinating briefings and reviews, taking minutes documenting decisions and action items, and tracking action items to completion.

Other Responsibilities

The responsibilities of all IRBs, acquisition review boards, and IPTs are fully described and maintained within their current charters. Also see Management Directive 2.8, "Integrated Information Technology/Information Management (IT/IM) Governance Framework," for the responsibilities of EA and the PMB and the NRC IT Asset Lifecycle Management Policy for the responsibilities of the IT Asset Manager for hardware and the Agency Software Manager.

CPIC Overview

The NRC CPIC is critical to the management and oversight of the agency's IT resources. It is key to the NRC's IT investment management because it provides a mechanism for delivering quality information and recommendations to executive decisionmakers on IT investments for inclusion into the IT portfolio. The NRC's IT investment management, comprised of the NRC's CPIC and IT budget processes, is part of the NRC's integrated IT/IM governance framework. The CPIC processes ensure that IT investments integrate and adhere to the framework's other disciplines:

- strategic planning and enterprise architecture
- project management methodology
- information and records quality principles

The NRC CPIC also ensures that IT investments are reviewed for compliance with cybersecurity internal standards and external standards mandated by NIST and Department of Homeland Security throughout their lifecycle and supports the CIO's involvement in relevant governance boards.

The NRC CPIC recognizes that IT investment management is dynamic. As such, IT investments are selected and continuously monitored and evaluated to ensure that each IT investment in the NRC IT portfolio effectively and efficiently supports the NRC mission and strategic goals. The NRC CPIC processes are designed to facilitate sound IT governance and the maturation of the NRC's IT investment management. The NRC CPIC model relies on three distinct, yet interdependent, set of processes: (1) select: (2) control; and (3) evaluate. An IT investment can be active concurrently in more than one CPIC process. After an IT investment is initially

selected and funded, it goes through the control and evaluate processes for review and reselection until it is determined that the investment has come to the end of its useful life. Upon this determination, the investment is decommissioned and removed from the portfolio.

Select

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

The select process and procedures capture IT investments and their supporting projects and IT resources for consideration in the overall IT portfolio. Investments under consideration include new investment proposals, as well as current investments being considered for reselection as–is or with enhancements. Investments being decommissioned also remain in the portfolio until they are completely removed from the production environment and require no more funding. These investments are captured, categorized, analyzed, prioritized, and either selected, denied, or placed on a lower priority or nonfunded list.

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

1. Support core or priority mission functions that need to be performed by the NRC.

2. Fill a performance or capability gap in achieving NRC strategic goals and objectives with the maximum benefits at the lowest lifecycle cost among viable alternatives.

3. Support a function that no alternative private sector or government source can more efficiently support.

4. 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.

5. Demonstrate a projected best value, based on an analysis of quantifiable and qualitative benefits and costs and projected return on investment, which is clearly equal to or better than alternative uses of available public resources.

    a. For best value, this may include improved mission performance in accordance with GPRAMA measures; reduced cost; increased quality, speed, or flexibility; and increased customer and employee satisfaction.

    b. IT investment costs shall be adjusted for such risk factors as the IT investment's technical complexity, the organization's management capacity, the likelihood of cost overruns, and the consequences of under- or non-performance.

6. Be consistent with applicable Federal and NRC enterprise and information architectures.

7. Reduce risk by employing measures such as avoiding or isolating custom-designed components to minimize the potential adverse consequences on the overall project; using fully-tested pilots, simulations, or prototype implementations before going into production; establishing clear measures and accountability for project progress; and securing substantial involvement and buy-in throughout the project from stakeholders.

8. Be implemented in phased, successive segments, modules, or other useful units as narrow in scope and brief in duration as practicable, each of which solves a specific part of an overall mission problem and delivers a measurable net benefit independent of future segments or modules.

9. Adhere to standards, including use of required artifacts, set forth in the NRC's project management methodology.

10. Adhere to security standards, including use of required artifacts.

11. Employ an acquisition strategy that allocates risk between government and contractor, effectively uses competition, ties contract payments to accomplishments, and takes maximum advantage of commercial technology.

Annually, all existing IT investments shall be reviewed and evaluated, based on data collected through the control process and procedures, and the results of evaluations performed through the evaluation process and procedures, to determine if they meet the following criteria for reselection and funding:

1. Continues to meet the business needs and expected performance goals.

2. Is capable of meeting business needs and expected performance goals with enhancements or modifications and is more cost effective than replacing the investment.

3. Mitigates risk effectively according to its current risk management plan and risk log. Includes the managing and closing of cybersecurity risks identified through continuous monitoring as listed on the investment's Plan of Actions and Milestones (POA&Ms).

4. Adheres to projected costs and expected benefits throughout the IT investment's lifecycle.

Control

The purpose of the control process and procedures is to ensure, as projects develop and investment expenditures continue, that the investment and its associated projects and activities continue to meet mission or business needs at the expected levels of cost and risk. The key objectives are (1) to ensure that corrective actions are taken quickly to address any deficiencies in project or operational components, and (2) to enable the NRC to adjust its objectives for an investment and appropriately modify expected outcomes if mission or business needs have changed.

The control process and procedures encompass various tools and techniques used to monitor and report on the risks associated with and performance of IT investments. These are key to

providing the quality data and information needed to monitor the status of projects' costs and schedules, status of risks (including POA&Ms), and performance of investments to make decisions on changes to investments, projects, or the portfolio. The control process and procedures include the annual major IT business case updates and submissions; major IT investment monthly reviews and CIO evaluations; quarterly investment and portfolio reviews; major IT investment control reviews; and CIO TouchPoints. Data and information collected during the monitoring of investments provide input into the evaluation of investments and support OMB reporting requirements.

Evaluate

The purpose of the evaluate process and procedures is to compare actual versus expected benefits and costs of investments and projects to determine return on investment, customer satisfaction, and value to the NRC in meeting mission and business needs. The key objectives are to:

- Assess the capacity of a project or investment to meet performance expectations within cost and schedule thresholds and in compliance with IT policies.
- Identify any needed changes or modifications to an investment (including 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 decisionmaking required to maximize the value of IT investments and the maturation of the IT portfolio and IT management practices. This entails analyzing the results of annual operational analyses, post implementation reviews, and as needed, TechStats. While each of these tools help inform the selection, reselection, and deselection of projects and investments within the IT portfolio, the operational analysis is paramount. NRC has based its operational analysis on the requirements set forth in the *Capital Programming Guide*, Section III, "Management In-Use." It provides a periodic, structured assessment of the cost, performance, and risk trends over time to help determine when cost and risk associated with an investment are no longer reasonable and outweigh the value received from the investment.