Capital Planning and Investment Control Policy and Process Overview

Office of Information Services
Capital Planning and Investment Control Team

Version 1.0

September 2015

Revision History

Date	Version	Summary of Changes	Author
09/28/2015	1.0	Updated IT CPIC policy and provided process overview to reflect FITARA and associated OMB requirements. Under FITARA, this policy is now publicly available. ADAMS Accession No. ML15247A497. Note: The NRC is maintaining detailed process and operating procedures in separate documents to support continuous refinement of the NRC's maturing investment management.	Vickie Smith, OIS/PMPD/IPMB Approved by Darren Ash, OEDO/DEDCM

Table of Contents

Background

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 (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 (PRA), 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 the CPIC process 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 Memorandum M-15-14, "Management and Oversight of Federal Information Technology," 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

[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.

upon and strengthen the CPIC requirements of CCA, FITARA establishes the Common 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 annual IT budget and capital planning guidance as part of OMB Circular A-11, "Preparation, Submission, and Execution of the Budget," and maintains its supplement, the "Capital Programming Guide" to assist agencies with the implementation of CPIC processes. OMB Circular A-130, "Management of Federal Information Resources," provides additional guidance. OMB updates these circulars based on current, relevant statues and Executive Orders. CCA, FITARA, and associated OMB 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 and provides an overview of the NRC's overarching CPIC process. It establishes the business rules and guidelines for consistency and compliance in executing the NRC CPIC process and procedures. This document has been updated to reflect FITARA requirements and, therefore, supersedes all previous CPIC policy and process documents. 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.

CPIC Policy

All NRC IT resources shall be managed in accordance with Federal mandates, OMB requirements, and agency procedures. Relevant to this policy are the following two definitions provided by OMB in Memorandum M-15-14:

"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 information technology 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 information technology not operated directly by the Federal Government.

"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 services 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.

OMB based this definition on the definition of information technology found in the CCA.

This policy establishes the following business rules and guidelines for the management and oversight of IT resources, including full time equivalents, under all IT investments (i.e., majors, non-majors, e-gov and multi-agency initiatives) unless stated as applying to only major IT investments:

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. IT investment refers to the expenditure of IT resources to enable core functions and processes that support the agency's mission and operational business requirements. An IT investment may include one or more project(s) for the development, modernization, enhancement, or maintenance of a single IT component or group of IT components with related functionality, and the subsequent operation of the component(s) in a production environment. All investments should have a defined lifecycle with start and end dates. The end date should represent the end of the currently estimated useful life of the investment based its components' most current alternative analyses or the results of the investment's most current operational analysis summarizing the operational performance of its components and the investment's ability to deliver required functionality.

3. 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[2].

4. 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 [3]
   - 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, "Financial Management Systems"
   - defined as major by the NRC's CPIC process

All other IT investments are considered non-major IT investments with the exception of e-gov and multi-agency initiatives used by the NRC. The NRC is a partnering agency to a number of e-gov and multi-agency initiatives 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.

5. 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."

6. 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.

---

[2] 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.

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

7. 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.

8. 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.

9. An IT investment shall facilitate interoperability, application portability, and scalability across networks of heterogeneous hardware, software, and telecommunications platforms.

10. Information systems and processes shall support interoperability and information accessibility, maximize the usefulness of information, minimize the burden on the public, and preserve the appropriate integrity, usability, availability, confidentiality, and disposition of information throughout the lifecycle of the information, in accordance with the PRA, Federal Information Security Modernization Act of 2014 (FISMA), Privacy Act of 1974 (as amended), and the Federal Records Act of 1950 (as amended).

11. Information systems and processes shall facilitate accessibility under the Rehabilitation Act of 1973, as amended; in particular, see specific electronic and information technology accessibility requirements, commonly known as "Section 508" requirements (29 U.S.C. § 794d).

12. For all IT investments, the NRC requires that records management functions and retention requirements be incorporated into the design, development, and implementation 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.

13. An IT investment shall have a committed Integrated Program Team (IPT) and charter, and all IT components and projects shall have an Integrated Project Team (IPT), charter, plan, and schedule.

14. All IT resources shall appropriately implement incremental development and modular approaches as defined in OMB guidance titled, "Contracting Guidance to Support Modular Development," issued June 14, 2012.

15. Decisions to improve, enhance, or modernize existing IT investments or to develop new IT investments shall be made only after conducting an alternative analysis that includes both Government-provided (internal, interagency, and intra-agency, where applicable) and commercially provided options, and the most advantageous option to the Government has been selected.

16. New IT acquisitions shall give preference 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. Decisions to acquire custom or duplicative solutions shall be justified based on overall lifecycle cost-effectiveness or ability to meet specific and high-priority mission or operational requirements.

17. IT needs shall be met through scalable, provisioned services when it is cost-effective to do so rather than acquiring or developing new information systems or equipment.

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 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 Deputy Executive Director for Corporate Management (DEDCM), who serves as the agency Chief Information Officer (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, and Compliance Programs (DEDMRT); and the DEDCM 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 National Institute of Standards and Technology (NIST).

Responsibilities of the DEDCM/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. Carry out the supervision, guidance, and coordination of the Director, Computer Security Office (CSO) who serves as the Chief Information Security Officer (CISO), and the Director, Office of Information Serves (OIS) who serves as the Deputy Chief Information Officer (DCIO).

3. Develop and implement an agencywide framework that includes policies, processes, and procedures for IT investment management, strategic planning and enterprise architecture (SP/EA), 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 Government Accountability Office, and is consistent with the NRC's overall planning, budgeting, and performance management programs.

4. Co-chair the executive level IT investment review board with the CFO, approve its membership, and approve revisions to its charter, as needed.

5. As co-chair of the executive level IT investment review board, the CIO, 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 IT investment review board, 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 subject matter experts (SMEs) in IT investment planning and management oversight, ensure agencywide coordination, and comply with CPIC requirements for IT investments, SP/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 Chair of the Strategic Sourcing Group, approve all acquisitions over $1 million, (including IT acquisitions) and provide oversight to acquisitions to ensure all IT 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. Recommend to the Commission any movement of funds for IT resources that requires Congressional notification.

14. Jointly with the Chief Human Capital Officer, 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.

15. Jointly with the DEDR and DEDMRT, 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. The CISO and the DCIO, who report directly to the DEDCM/CIO, are the DAAs for all non-major systems.

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 IT investment review boards.

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 enterprise architecture (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 Office 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 OIS and with CSO 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 project managers 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 project managers.
12. Set 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 IT investment review boards, acquisition review boards, and IPTs are fully described and maintained within their current charters.

CPIC Process

The NRC CPIC process 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 providing quality data and recommendations to executive decision-makers 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 process ensures 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 process also ensures that IT investments are reviewed for compliance with cybersecurity internal standards set forth by CSO 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 process 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 process is 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, processes:

- select process
- control process
- evaluate process

An IT investment can be active concurrently in more than one CPIC process. After the IT investment's initial funding in the select process, 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 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 those IT investments and projects that will best support mission needs.

The select process captures 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:

- Support core or priority mission functions that need to be performed by the NRC.
- 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.
- 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, which is clearly equal to or better than alternative uses of available public resources.
    - 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.
    - 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.
- Be consistent with applicable Federal and NRC enterprise and information architectures.
- 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.
- 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.
- Adhere to standards, including use of required artifacts, set forth in NRC's Project Management Methodology.
- Adhere to standards, including use of required artifacts, set forth by CSO.
- 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 the results of evaluations performed through the evaluation process, to determine if they meet the following criteria for reselection and funding:

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

- 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&M).

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

Control

The purpose of the control process 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 encompasses the tools and techniques used to monitor and report on the risks associated with and performance of IT investments. This process is key to providing the information needed to evaluate 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 includes the monthly review and CIO evaluations and reporting on major IT investments to OMB through the Federal IT Dashboard; annual control reviews and CIO TouchPoints; annual major IT business case updates and submissions; and the management of performance baselines of major IT investments. 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 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 encompasses the tools and techniques associated with the review and analysis of IT investments and the decision-making required to maximize the value of those investments. These include the annual operational analysis, the post-implementation review, and the TechStat. While each of these tools will 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 *Section III,*

Management In-Use of the “Capital Programming Guide.” 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.