# INFORMATION DIRECTIVE
# PROCEDURE

| System Life Cycle Management (SLCM) Procedure | | |
|---|---|---|
| Directive No.:<br>CIO 2121-P-03.0 | CIO Approval: 12/21/2017 | Transmittal No.: 12-004* |

*Issued by the EPA Chief Information Officer,*
*Pursuant to Delegation 1-19, dated 07/07/2005*

## System Life Cycle Management (SLCM) Procedure

### 1. PURPOSE

This procedure defines the requirements and processes for implementation of EPA's System Life Cycle Management (SLCM) Policy.

This SLCM Procedure establishes EPA's (Agency) approach and practices in the pre-definition, definition, acquisition/development, implementation, operations and maintenance, and termination of EPA information technology (IT) systems and applications.

This procedure provides guidelines to assist the system owners, system managers and project managers in:

- Making information system governance decisions to adhere to the SLCM Policy. The SLCM Policy must be implemented in conjunction with existing EPA policy and procedures for Enterprise Architecture (EA), Capital Planning and Investment Control (CPIC), and Information Security requirements.
- Tailoring system life cycle management activities to meet various IT systems and application needs while maintaining adequate management controls.

### 2. SCOPE

This SLCM Procedure outlines the required SLCM phases, steps, and activities for the individuals responsible for the pre-definition, definition, acquisition/development, implementation, operations and maintenance, and termination of EPA IT systems and applications. This procedure also details the set of SLCM documents that are necessary to properly manage and control EPA IT systems and applications based on the size, scope and complexity of the system. Project Managers and System Managers will use this procedure to determine the complete set of documents required for an information system based on the results of system life cycle tailoring activities.

This policy applies to all EPA IT systems and application projects, both applications and general support systems (GSS). It is applicable to custom developed, commercial-off-the-shelf (COTS), or government-off-the-shelf (GOTS) projects and applies to applications developed for mobile devices. It also applies to systems developed on behalf of EPA by contractors irrespective of where the IT systems are hosted; including cloud-based solutions. Small desktop applications (i.e. spreadsheets) are excluded from the requirements of this policy.

The specific SLCM documents, participants in the life cycle process, and the necessary reviews and approvals vary from system to system. The guidance provided in this document should be tailored to the individual project based on cost, complexity, and criticality to the agency's mission. To ensure documentation requirements are not overly burdensome, the SLCM documents should be tailored according to the scope of the effort.

| System Life Cycle Management (SLCM) Procedure | | |
|---|---|---|
| Directive No.:<br>CIO 2121-P-03.0 | CIO Approval: 12/21/2017 | Transmittal No.: 12-004* |

## 3. AUDIENCE

The audience for the policy includes all EPA and contractor personnel participating in the development and management of IT systems, including but not limited to:

- Chief Information Officer (CIO)
- Chief Financial Officer (CFO)
- Chief Technology Officer (CTO)
- Senior Information Officials (SIOs)
- Information Management Officers (IMOs)
- Information Security Officers (ISOs)
- Information System Security Officers (ISSOs)
- System Sponsors
- System Owners
- System Managers
- Project Managers (PMs)

## 4. BACKGROUND

The SLCM Procedure provides for the integration of system life cycle management with IT investment management practices, Enterprise Architecture, quality, accessibility and information security requirements. Laws and federal requirements - in particular the Clinger-Cohen Act of 1996, the Federal Information Security Management Act of 2002 (FISMA), and Office of Management and Budget (OMB) Circulars A-11 and A-130 - require EPA to ensure that its life cycle management procedures are comprehensive and up-to-date. EPA's SLCM Procedure satisfies applicable federal laws and regulation requirements. This procedure also takes into account industry best practices for software development including standards from the Information Systems Audit and Control Association (ISACA), http://www.isaca.org/Knowledge-Center/Standards/Pages/default.aspx.

A comprehensive approach to SLCM ensures that EPA IT systems and applications are properly planned and managed, controllable, cost-effective, and support the mission and business goals of the Agency. It also reduces the risk of failed systems for all applications and general support systems.

The six phases of the System Life Cycle (SLC) are Pre-Definition, Definition, Acquisition/Development, Implementation, Operations and Maintenance, and Termination. During each phase SLCM documentation is created, updated or modified. The tasks and documents for each phase are described in this procedure. Not every project will require the phases to be sequentially executed; however, the phases are interdependent. Depending upon the size and complexity of the project, phases may be combined or may overlap.

Five Control Gate reviews during the SLC provide management control and direction, decision- making, coordination, confirmation of successful performance of activities, and determination of a system's readiness to proceed. Requirements that must be met at these control gates include those for Enterprise Architecture (EA), Capital Planning and

Investment Control (CPIC), Information Security and SLCM.

While the SLCM is primarily phase-driven, requiring work products on a schedule developed and maintained by the System Manager, certain SLCM-related reporting requirements have a calendar based reporting schedule. Most of these items support the CPIC, EA and Information Security policies. These items should be incorporated into the Project Managers schedule.

Figure 1 provides an overview of the SLCM process detailed in this procedure.

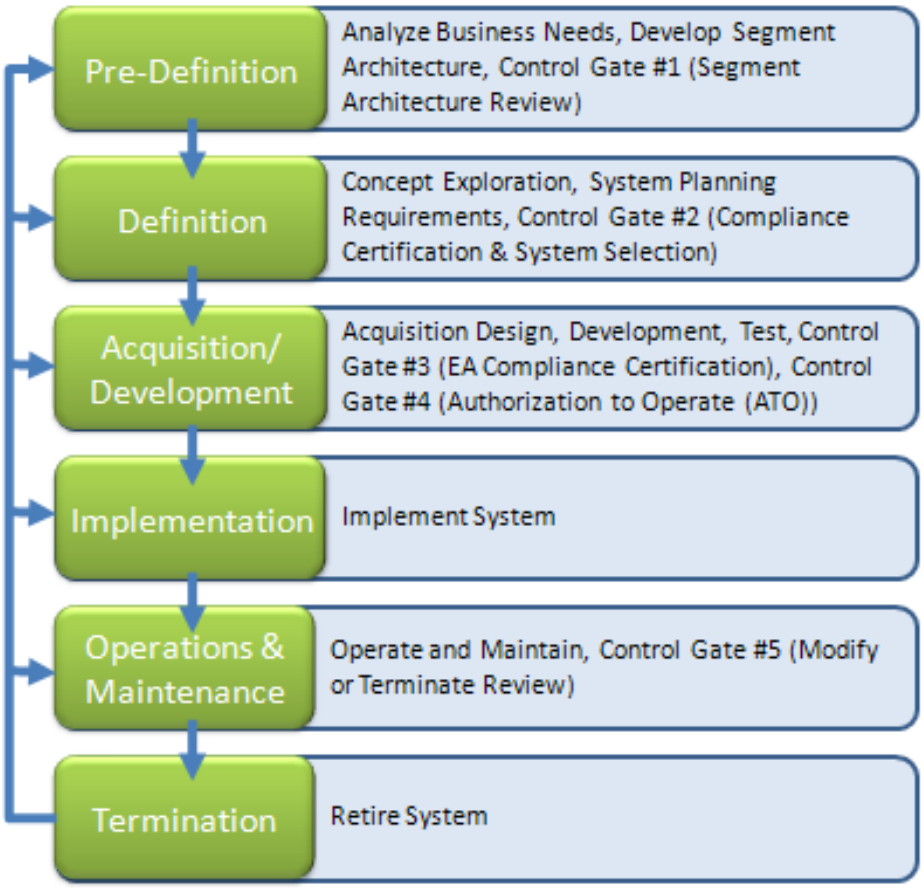



**Figure 1 EPA System Life Cycle Management Framework**

| System Life Cycle Management (SLCM) Procedure | | |
|---|---|---|
| Directive No.:<br>CIO 2121-P-03.0 | CIO Approval: 12/21/2017 | Transmittal No.: 12-004* |

## 5. AUTHORITY

Authority to issue this procedure derives from EPA's System Life Cycle Management Policy. The authorities listed in the SLCM Policy also support this SLCM Procedure.

## 6. PROCEDURE

The SLCM procedure describes the activities, documents, and reviews that are necessary to meet SLCM requirements. The activities described in the SLCM Procedure address all types of systems and application, and therefore require tailoring in order to apply only those activities applicable to specific systems. This procedure provides System Managers and System Owners the flexibility to determine the life cycle activities and accompanying processes necessary to address the needs of their specific projects.

### 6.1 System Development Tailoring

SLCM tailoring allows System Managers to adjust the system development methodology described in the EPA SLCM procedure to address the size, scope, complexity, and constraints of their specific projects. Tailoring determines the level of rigor and documentation required to manage a system development project based on the size, scope, and complexity of a project. After selecting a specific tailoring schema, tailoring decisions become part of the project baseline and System Managers must successfully complete the system change control process before implementing changes to previously accepted tailoring decisions.

As part of tailoring, System Managers and System Owners will need to determine the methodology to use to develop their project based on the unique factors specific to their information system. Common development methodologies include but are not limited to: Waterfall, Agile, Rapid Application Development (RAD) or Iterative approach, Rational Unified Process (RUP), and Spiral. A project may also have a mixed life cycle, where one component of the system is in a different phase from other system components. It is appropriate to use this SLCM Procedure tailored to suit information system needs regardless of the selected development methodology. When developing a tailoring plan System Managers should analyze all SLCM requirements to determine which are necessary for their system, which can be combined or consolidated with another requirement, and the level of detail that will be necessary for the requirements that are selected as part of the plan.

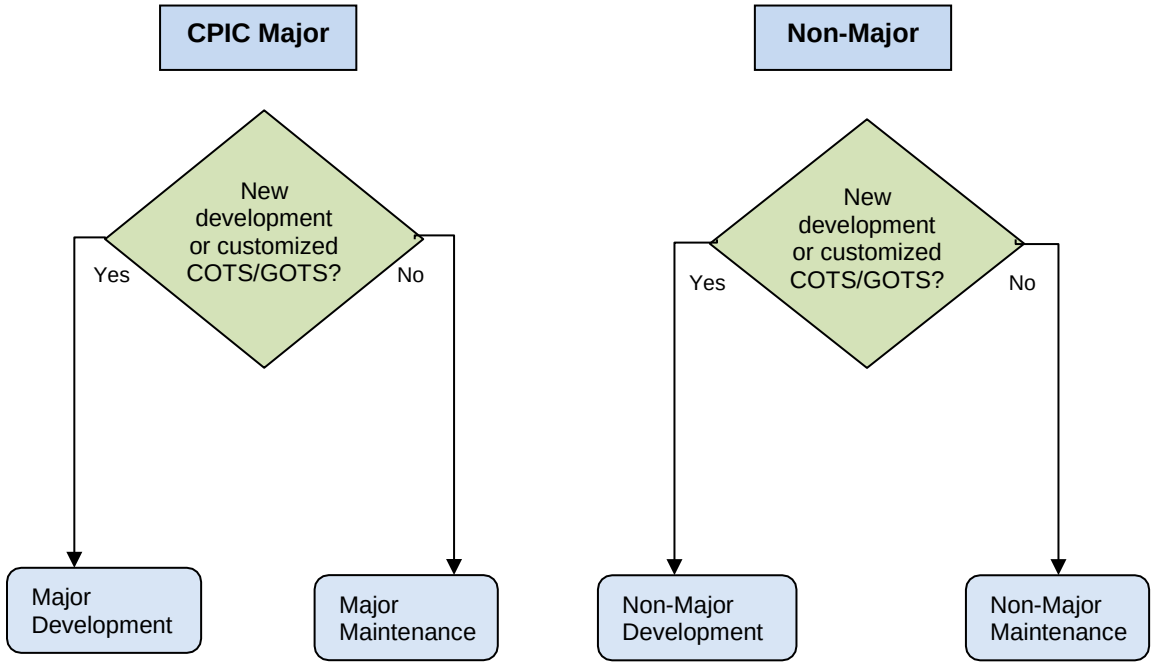
EPA uses several factors to determine how to tailor a system's development. These factors include:

- Size of investment
- Build-versus-buy approach
- Agency risk
- Development methodology

Figure 2 provides a recommended decision path to tailor EPA systems. The decision path defines four system type recommendations:

1. Major Development (details discussed in Appendix A)
2. Non-Major Development (details discussed in Appendix B)
3. Major Maintenance (details discussed in Appendix C)
4. Non Major Maintenance (details discussed in Appendix D)

A detailed appendix for each system type will assist System Owners and Project Managers in determining what SLCM documents apply to their specific system, and which documents are required to pass through each Control Gate. The lists provide the documentation that should be considered by the Project Manager and System Manager. However, a specific requirement may not be applicable for your system or the level of detail needed to meet the requirement may be minimal based on your tailoring approach. Although variances exist, each SLCM phase must be completed for all EPA systems.




CPIC: Capital Planning and Investment Control
COTS/GOTS: Commercial-off-the-Shelf / Government-off-the-Shelf

**Figure 2 EPA System Life cycle Management Tailoring Decision Tree**

### 6.1 Pre-Definition Phase

The Pre-Definition Phase is where business owners determine if an IT System or Solution is needed to fulfill a business need and/or performance gap in any of EPA's functional areas including but not limited to administrative, financial, technological, or scientific functions. Upon completion of this phase, an organization has agreed that there is a business need and/or performance gap that requires a system to fulfill it, and that this

system fits into the related Segment Architecture of the organization. The phase begins when the Senior Information Official for an organization meets with business owners (*those responsible for identifying the need for which an IT solution may fulfill, later in the process they will typically become the system owners*) to analyze and document the business processes, data flows, and associated performance measures. Solutions advance to the Definition phase when all Control Gate 1 documentation has been completed and approved by the System Owner and Chief Architect or designee. *

Control Gate 1 – Documentation**:

1. Segment Architecture Charter
2. Segment Architecture
3. Segment Performance Measures
4. Control Gate 1 Decision Memo (must include the documented business or mission need)

** It is possible that if business and IT owners determine that an IT system is not the appropriate solution for the identified business need, then no further SLCM activities are required.*

***If it is a system migration or upgrade, then the Decision Memo is the only CG 1 document required*.

### 6.2 Definition Phase

The Definition Phase establishes the business justification for the system and a concrete plan for implementation or acquisition. Upon completion of this phase, the organization responsible for the system has approved the project concept, approved funding to proceed, and drafted the system tailoring plan. For mobile apps, completion of this phase includes concept approval by the Mobile Access Review Committee (MARC) - detailed in Appendix E. The phase begins when an organization issues a formal approval to explore the need for a system and concludes when the organization has formal approval to proceed with system development. This phase is where essential IT planning begins revolving around the EA and information security. The information security activities ensure that Agency information will be properly protected and available only for appropriate uses. During this phase, IT Investment Management and EA activities aim at ensuring the intended systems will support Agency requirements without unnecessary redundancy. These activities ensure that system developers and managers properly manage EPA resources in the IT environment. During this phase Project Managers should reference GAO's Cost Estimating and Assessment Guidance - http://www.gao.gov/new.items/d093sp.pdf.

#### Definition Phase Steps and Activities

For every approved IT system, System Sponsors must allocate sufficient resources to execute the project. The following steps and activities are performed as part of the Definition Phase by the System Owner, System Manager and Project Manager.

#### Step 1: Concept Exploration

- Identify and establish the business justification for the proposed system
- Establish the project sponsorship/ownership
- Consider the project team needs
- Document the exploration activities
- For mobile apps, submit the appropriate mobile app concept review form to MARC as

detailed in Appendix E. Mobile app development may not begin without approval from MARC
- Complete CROMERR documentation if applicable
- Review and approve to proceed to the next phase
- Initiate security planning activities

**Step 2: System Planning**

- Refine the acquisition strategy
- Analyze the project schedule
- Staff the Project Team
- Develop the Project Management Plan (PMP)
- Review the feasibility of system alternatives
- Study and analyze security implications
- Tailor the SLCM and document the tailored decision path in the PMP

**Step 3: Define Requirements**

- Further define and refine functional and data requirements
- Complete business process engineering of the functions to be supported
- Develop detailed data, data exchange and process models
- Define functional and system requirements that are not easily expressed in data and process models, including the requirements of the business process, user requirements, and operational requirements
- Refine the high-level system architecture and logical design to support the system and functional requirements
- Develop conceptual solution architecture
- Add system to the Agency's system registry
- Coordinate with enterprise services (e.g. CDX, registries)
- Continue to identify and mitigate risk that the technology can be phased in and coordinated with the business

**Step 4: Conduct Control Gate #2 – EA Compliance Certification and System Selection Review**

This control gate ensures that the Concept Proposal is sound, that it does not conflict with the Enterprise Architecture, and that the proposed project is viewed as a good investment for the Agency.

For CPIC Major Investments, the SIO approves the IT Investment Business Case for addition to the Agency's IT Investment Portfolio. The Project Manager and System Manager perform an initial EA Compliance Certification Review in coordination with the Chief Architect. The Project Manager and Senior Information Official (SIO) forward the business case to the Quality and Information Council (QIC), who relies on the Information Investment Subcommittee (IIS) to provide a thorough business case review in accordance with the Agency's CPIC Select Phase criteria. The IIS then forwards its investment recommendation to the QIC for its final decision.

For Non-major systems, the SIO approves the concept proposal and business case. The Project Manager and System Manager perform an initial EA Compliance Certification Review. The Project Manager forwards the reviewed package to the Senior Information

Official (SIO), who will decide whether the project can continue to the Acquisition/ Development Phase.

During this Control Gate, System Mangers must ensure a check of proposed technologies against the Agency IT Standards Profile; non-standard technology may require an IT waiver. For mobile apps, concept approval from MARC is required and must be included in the review package.

**Definition Phase Review**

The Definition Phase Review is performed at the end of the phase, which ensures that the Concept Proposal is approved before proceeding to the next phase. The Project Manager should present to the System Owner a management review or checkpoint at the completion of the Definition Phase to measure progress. Checkpoints are high-level milestones. The System Owner should use the briefing to approve the completion of the phase and to make a go/no-go decision whether to proceed with the project. The review ensures that the plans developed during the definition phase meet the project objectives in the time and budget requirements set by the System Owner. For mobile apps, concept proposals must be approved by MARC before any development can begin.

**Definition Phase SLCM Documents**

Project Managers should use Figure 2 to determine which path is appropriate for their system, and then review the appendix that outlines the necessary documents for that path.

### 6.3 Acquisition/Development Phase

The Acquisition/Development Phase results in the acquisition or development of the system that satisfies the mission need defined in the business case justification established in the Definition Phase. The Clinger-Cohen Act of 1996 suggests that agencies evaluate the possibility of using commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) products, and to use them when practical. However, systems based on COTS or GOTS products may require some degree of modification, integration, and/or customization prior to implementation. Since that work must be properly documented and controlled, it must adhere to the entire SLCM procedure and any additional applicable procedures and standards.

The testing and certification of security also begins in this phase. System managers must work with their Information Security Officers and Information System Security Officers to ensure that security requirements and controls are properly met; this includes necessary NIST requirements. Additionally, if the application will be hosted in a Cloud-based environment the system must adhere to the additional controls published by FedRAMP (http://www.gsa.gov/portal/category/102371). Testing ensures the integrity of data and confidentiality mechanisms in COTS/GOTS products or custom- designed systems.

**Acquisition/Development Phase Steps and Activities**

The Project Manager and System Manager ensure the following activities are performed as part of the Acquisition/Development Phase. The Project Manager works with the ISO and ISSO to refine and update the security requirements. The Project Manager also ensures development of the Contingency plans and/or Continuity of Operations plans (COOP) and the reporting of CPIC requirements, if applicable. *EA Control Gate #3 – EA Compliance Certification* is required during this phase. *EA Control Gate #4 – Authorization*

*to Operate* is required at the end of this phase. Across each activity, previous SLCM documents should be evaluated and updated as appropriate to take into account details identified as the information system is better defined.

During the Acquisition Phase, the System Manager, System Owner, and other key stakeholders will determine if they will develop a custom solution, leverage a COTS/GOTS solution, or use a hybrid solution that involves heavy customization of a COTS/GOTS product. This decision is an important part of the development process that may involve conducting an alternatives analysis or cost/benefit analysis to reach the most appropriate decision for the information system project.

If a COTS/GOTS product is selected, the Project Manager and System Manager will document how and if the vendor's documentation will be used to satisfy the requirements of the SLCM procedure in the Project Management Plan.

**Step 1: Acquisition**

This step is completed if the project has been selected to conduct an acquisition. If an acquisition is not required, this step can be omitted.

- Make management decisions concerning procurement of government resources and services and contractor services, including ensuring the availability of funding
- Preparing Requests for Proposals
- Perform technical analysis and evaluation of vendor proposals
- Make request for bid and conduct source selection
- Make contract award

**Step 2: Design**

- Develop the System Design Document
- Identify the target environment, development environment, and the design environment
- Design the Conversion/Migration/Transition Plan
- Develop the Sequencing Plan
- Conduct the security risk assessment
- Develop the Contingency Plan

**Step 3: Conduct Control Gate #3 – EA Compliance Certification Review**

The EA Compliance Certification Review ensures that the system's design conforms to the planned solution architecture and continues to address the business need while remaining in alignment with the Agency EA.

The Chief Architect will conduct the EA Compliance Certification Review for all Major systems, certifying that solution architectures developed for information management and technology development, modernization, and enhancement, are compliant with the Enterprise Architecture. The SIO, or IMO if delegated, conducts the EA Compliance Certification Review and certifies architecture compliance for Non-Major systems. For Major systems, the Chief Architect certifies the solution architectures as architecturally compliant prior to project development unless the System Manger obtains the appropriate waivers.

For most non-Major systems the System Owner must certify the solution architecture or obtain the appropriate waivers.

**Step 4: Development**

- Code and test software
  - Integrate software
  - Conduct software and system testing
  - Install software
  - Document software acceptance

For COTS/GOTS products, some tasks and activities may have been performed by the vendor or providing department or agency. In those cases, the product documentation may be appropriate to meet EPA SLCM document requirements. The project manager must document the extent to which product or contract deliverables will be used to satisfy EPA SLCM requirements.

**Step 5: Test**

- Establish the test environment
- Conduct integration tests
- Conduct subsystem/system testing
- Conduct security testing
- Conduct acceptance testing

**Step 6: Conduct Control Gate #4 – Authorization to Operation (ATO) Review**

For general support systems and Major applications, the Authorization to Operate (ATO) Review ensures that the system is ready to move into an operational state. The SIO conducts the Authorization to Operate Review using the certification package to determine the appropriateness of allowing the system to move into an operational state. The Project Manager coordinates with key stakeholders including the Information Security Officer and the Information System Security Officer to ensure the certification package is completed and there is an approved Authorization to Operate as part of the Risk Management Framework (if applicable). The IMO makes the final recommendation and then forwards the certification package to the SIO for final approval.

The system must be accredited for operations prior to its being moved into an operational state. The SIO can provide full authorization to operate or denial of authorization to operate. Non-major systems generally have their security proved as part of the general support system. Therefore, each GSS will have application deployment requirements to ensure integrity of their security and consideration in their maintenance scheme.

**Acquisition/Development Phase Review**

The Project Manager performs a review at the end of the Acquisition/Development Phase. The review ensures that the System Manager identifies the requirements of the system and establishes the feasibility of the system. The review includes the products of the Acquisition, including the Acquisition Plan and the requirements specifications. The System Manager organizes, plans, and leads this review; submitting documentation of the review to the System Owner for approval.

**Acquisition/Development Phase SLCM Documents**
Project Managers should use Figure 2 to determine which path is appropriate for their system, and then review the appendix that outlines the necessary documents for that path.

### 6.4 Implementation Phase

This phase results in the establishment of the completed system or system modifications into the production environment. Activities may include installing hardware and/or software into the production environment, data conversion, user training, and a post-implementation review. The System Implementation Plan, completed during this phase, must include configuration and implementation requirements that ensure that System Managers and Project Managers implement and test the system as specified in the prior phase.

The system being implemented can fall into three categories: (1) replacement of a manual process, (2) replacement of a legacy system, or (3) upgrade to an existing system. Regardless of the type of system, all aspects of the implementation phase should be followed. Variations in the steps that are followed, however, may be required as part of the Application Deployment Checklist (ADC), if applicable.

**Implementation Phase Steps and Activities**

During this phase, the developers install the system or system modifications and make them operational in the production environment. The Project Manager initiates this phase after the user has tested and accepted the system. Activities include notification of implementation to end users, execution of the previously defined training plan, data entry or conversion, completion of security certification and accreditation, and post-implementation evaluation. This phase continues until the system is operating in production in accordance with the defined user requirements.

**Step 1: Implement System**

The Project Manager ensures the following activities are performed:

- Notify users of implementation
- Execute the Training Plan
- Perform data entry or conversion
- Deploy system and complete Application Deployment Checklist (ADC) – *if applicable*
- For native mobile apps, MARC will assist the Project Manager with deployment to third-party app stores for which EPA has a signed Terms of Service (TOS)

**Implementation Phase Review**

The System Manager conducts a post-implementation review to ensure that the system functions as planned and expected; to verify that the system cost is within the estimated budget; and to verify that the intended benefits are derived as projected. Normally, this is a one-time review, occurring after a major implementation, although it may also occur after a major enhancement to the system. The results of an unacceptable review are submitted to the System Owner for review and follow-up actions. The System Owner may decide it is necessary to return a deficient system to the responsible System Manager for correction of deficiencies.

During the Implementation Phase review, recommendations may be made to correct errors, improve user satisfaction, or improve system performance. For contractor development, the Project and System Managers will perform analysis to determine if additional activity is within the scope of the statement of work or acquisition package.

**Implementation Phase SLCM Documents**

Project Managers should use Figure 2 to determine which path is appropriate for their system, and then review the appendix that outlines the necessary documents for that path.

### 6.5 Operation and Maintenance (O&M) Phase

This phase ensures that the system operates properly in its production environment and that maintenance takes place. During this time, the Project Manager and System Manager maintain schedules and periodically conduct reviews to ensure the health of the system and to validate its suitability for meeting the business requirements. The System Manager uses structured techniques to detect defects, capture user satisfaction, review the system requirements, and evaluate the suitability of existing and emerging technologies to continue to meet the mission need.

**O&M Phase Steps and Activities**

During this phase, activities can include performing routine maintenance in accordance with manufacturer's guidelines, installing patches and/or updates to system components, and making enhancements consistent with user needs/desires and consistent with the mission need. Major new requirements or significant technology refreshment may cause maintenance that requires the system to return to the Definition or Acquisition/Development phase. For enhancements to existing mobile apps, contact MARC to determine whether a new concept proposal is required.

While all updates and other maintenance activities require some review and update of documentation created in the Acquisition/Development phase, occasionally these needs require more extensive changes, which could require a formal reiteration through the Definition and Acquisition/Development phases. It is also possible that contemplated changes are so extensive that it is not economical to continue to support the existing system.

**Step 1: Operate & Maintain**

- Identify systems operations
- Maintain data/software administration
- Identify problem and modification process
- Maintain system/software maintenance
- Maintain system documentation
- Periodic Security Reviews and Risk Assessments

**Step 2: Conduct Control Gate #5 – Modify or Terminate Review**

The Modify or Terminate Review determines if the IT Investment should continue to be modified, or be terminated. For Major systems and select Non-Major systems, the Modify or Terminate Review will coincide with the annual IT investment review. The SIO forwards the review package to the QIC, who relies on the IIS to provide a thorough Business Case Review in accordance with the Agency's CPIC Evaluation Phase criteria to determine if the IT investment or information system can optimally continue to support mission/user requirements

and the Agency's strategic direction. The IIS develops recommendations for the QIC to make a decision on whether to keep this investment as part of the Agency's IT Investment Portfolio as it stands or to modify or terminate it.

For most Non-Major systems the control gate will be coordinated by the System Manager annually or at a frequency that is appropriate for the scope and size of the system. The frequency of the review should be documented in the PMP or the System Implementation Plan. The system manager and IMO provide a recommendation to the SIO for approval to maintain, modify or terminate the system.

**O&M Phase SLCM Documents**

Project Managers should use Figure 2 to determine which path is appropriate for their system, and then review the appendix that outlines the necessary documents for that path.

### 6.6 Termination Phase

This phase results in removing an existing system from the production environment at the end of the life cycle process. During this phase, the System Managers retire and close down systems that have been declared redundant or obsolete. Occasionally, a System Manager will use this phase to shut down a major subsystem while the main system remains in operation. The emphasis of this phase is to ensure the packaging and archiving of data, procedures, and documentation in an orderly fashion to make it possible to reinstall the system and bring it back to operational status, if necessary, and to retain all data records in accordance with EPA policies regarding retention of electronic records. This phase represents the end of the system life cycle.

The system retirement activities preserve information not only about the current production system but also about the evolution of the system through its life cycle.

**Termination Phase Steps and Activities**

This phase ends the operation of the system in a planned, secure, orderly manner, including archiving system components and data or incorporating them into other systems as required, and securely disposing of hardware and software as appropriate. The System Owner and System Manager ensure the following activities as part of the *Termination Phase:*

Step 1: **Retire System**

- Prepare retirement and disposition plans
- Archive or transfer data
- Archive or transfer software components
- Sanitize and dispose of equipment/hardware and software media (including system backup and other media)
- Prepare the post-termination review report

**Termination Phase Review**

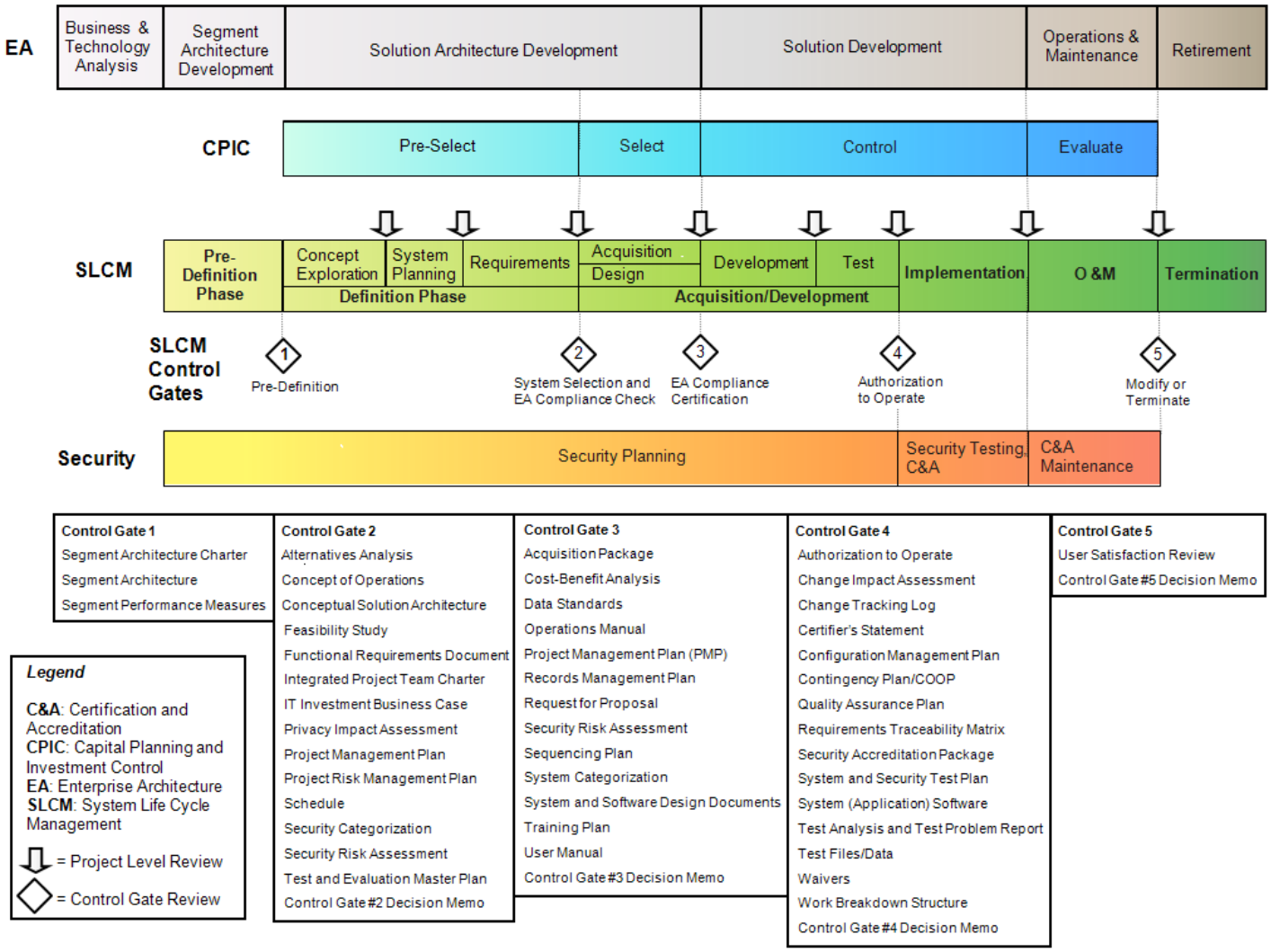
The System Manager performs the Post-Retirement Review within six months after retirement of the system to notify all parties of the final shutdown of the system. The Post-Retirement Review Report also documents the lessons learned from the shutdown and archiving of the terminated system.

### Termination Phase SLCM Documents

Project Managers should use Figure 2 to determine which path is appropriate for their system, and then review the appendix that outlines the necessary documents for that path.

## 6.7 Information Systems Life Cycle Management Framework

EPA's Information Systems Life Cycle Management Framework facilitates the identification, planning, and implementation of IT systems by integrating EA, CPIC, SLCM, and Security lifecycles. Figure 3 (below) illustrates their alignment.




*Note: This is a comprehensive list of Control Gate documents. Not all documents are required for every system. Refer to Section 6.01 and the corresponding Appendix for the specific requirements for your system type.*

| System Life Cycle Management (SLCM) Procedure | | |
|---|---|---|
| Directive No.:<br>CIO 2121-P-03.0 | CIO Approval: 12/21/2017 | Transmittal No.: 12-004* |

## 7. ROLES AND RESPONSIBILITIES

In support of the SLCM Policy, this procedure includes roles and responsibilities related to the SLCM phases.

Roles with significant responsibilities necessary for implementing the EPA SLCM Procedure include the following:

**Chief Information Officer (CIO)**, who also is the Assistant Administrator for the Office of Environmental Information, is responsible for:

- Approving the SLCM Policy
- Ensuring Agency compliance with the SLCM Policy and Procedure by providing guidance and tools to senior level managers for program oversight
- Deciding on waiver requests to the SLCM Policy
- Delegating review and approval of any waivers to the SLCM Procedure to the CTO

**Assistant Administrators, Chief Financial Officer (CFO), General Counsel (GC), Inspector General (IG), Deputy Chief of Staff to the Administrator, Associate Administrators, and Regional Administrators and Laboratory Directors are responsible for:**

- Ensuring compliance with SLCM requirements for IT systems within their organizations

**Chief Technology Officer (CTO)** is responsible for:

- Establishing and publishing procedures, technical operational procedures and standards (TOPS), and guidance supporting the Agency's SLCM Policy
- Reviewing and approving waivers to the SLCM Procedure

**Office of Technology Operations and Planning (OTOP) Director** is responsible for:

- Maintaining the SLCM Policy, the SLCM Procedure, and supporting documents and tools
- Monitoring compliance with the SLCM Policy and Procedure through EA, IT Investment Management, and security processes

**Chief Architect** is responsible for:

- Leading the development and maintenance of the Agency's Enterprise Architecture (including target architecture, transition strategy, and enterprise transition plan) in conjunction with the SLCM Policy and Procedure
- Certifying and providing guidance for compliance of solution architectures during EA reviews
- Reviewing and approving Control Gates 1, 2, and 3, for Major Systems and Non-major Systems as appropriate.

**Director of the Office of Acquisition Management (OAM)** is responsible for:

- Ensuring the incorporation of EPA's SLCM requirements in requests for proposals and contracts as appropriate

**Senior Information Officials (SIOs)** are responsible for:

- Apprising the Quality and Information Council (QIC) of major SLCM issues within their offices
- Ensuring compliance with SLCM Policy and Procedure for systems within their offices
- Ensuring that the information technology used and managed by their organization supports its business needs and mission and helps to achieve strategic goals
- Ensuring EA Compliance of solution architectures
- Reviewing, concurring, advising and/or submitting on waiver requests to the SLCM Policy and Procedure, as applicable
- Approves a project to continue through control gates (this may be delegated for smaller systems)
- Meeting with business and system owners to ensure development and management activities are completed in compliance with Agency policy

**System Sponsors** are responsible for:

- Authorizing, approving, and ensuring adequate funding and resources during the system life cycle of their information systems
- Appointing System Owners and authorizing those individuals to initiate system development
- Reviewing waiver requests

**System Owners** are responsible for:

- Monitoring compliance to the SLCM Policy and Procedure including approving Tailoring Plans
- Concurring on waivers from the SLCM policy and/or procedure, as applicable
- Appointing Project Managers and System Managers
- Serving as the information owner of the system
- Coordinating SLCM development activities with those of the EA, IT Investment Management, and information security processes
- Ensuring compliance to Section 508 requirements during the SLCM
- Approving completed Control Gate and Project Level Reviews

**System Managers** are responsible for:

- Developing the SLCM Tailoring plan
- Providing day-to-day management of the system life cycle process and products within their programs
- Ensuring that systems properly advance through the SLCM phases and activities
- Recommending and preparing written justification for waivers and documenting them as part of the Project Management Plan
- Preparing Control Gate and Project Level Reviews

**Project Manager (PM)** is responsible for:

- Managing the defined system through development to delivery
- Incorporating the SLCM documents and work products in the system project schedule
- Assigning resources on the system project team to complete SLCM Documents
- Works with the System Manager to prepare Control Gate and Project Level Reviews

**Information Management Officers (IMOs)** are responsible for:

- Supporting the SIO in ensuring compliance with this policy and the SLCM procedure for systems within their office
- Reviewing SLCM documentation
- Reviewing and concurring on waiver requests to the SLCM Procedure, as applicable

**Information Security Officers (ISOs)** are responsible for:

- Reviewing and supporting the development of security SLCM artifacts, as appropriate
- Assigns security responsibilities throughout the system life cycle

**Information System Security Officers (ISSOs)** are responsible for:

- Maintaining the operational security of the information system
- Assisting in the planning and execution of security related SLCM documentation

**Privacy Act Officer** is responsible for:

- Reviewing and supporting system development and management as it relates to privacy and personally identifiable information

**Mobile Access Review Committee (MARC)**, comprised of members from Office of Web Communications, Office of Information Analysis and Access, Office of General Counsel, and the OEI Lead Region and subject matter experts as needed, is responsible for:

- Reviewing and approving mobile app concept proposals
- Providing guidance for mobile app development
- Assistant in the deployment of native mobile apps to third-party app stores

## 8. RELATED INFORMATION

DOCUMENTS

- CIO Policy 2130.1, Section 508: Accessible Electronic and Information Technology (EIT) February 20, 2014.
- CIO 2130-P/S/G-01.0 Accessible Electronic and Information Technology Standards, Procedures, and Guidance

| System Life Cycle Management (SLCM) Procedure | | |
|---|---|---|
| Directive No.:<br>CIO 2121-P-03.0 | CIO Approval: 12/21/2017 | Transmittal No.: 12-004* |

POLICIES, STANDARDS AND GUIDANCE

- Capital Planning and Investment Control (CPIC) Policy: http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/2120.pdf
- Capital Planning and Investment Control (CPIC) Procedures for the Office of Management and Budget (OMB) Exhibit 300: *http://intranet.epa.gov/cpic/fy2008/cpic-procedures- sept05.pdf*
- Data Exchange and Collection Procedure: http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/CIO_2122-P-04.0.pdf
- Data Standards Policy: http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/2133.0.pdf
- Enterprise Architecture Procedure: *http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/ea- procedure-final040406.pdf*
- EPA Acquisition Regulation (EPAAR): *http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?sid=52c48b59c02b4481b8576a658c6e69ab&c=ecfr&tpl=/ecfrbrowse/Title48/48cfrv6_02.t pl*
- EPA's Earned Value Management Procedures: http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/2120-p-01.1.pdf
- EPA System Life Cycle Documents Guidance (URL TBD)
- Federal Cloud Computing Strategy: http://www.cio.gov/documents/federal-cloud-computing- strategy.pdf
- FedRAMP: http://www.gsa.gov/portal/category/102371
- GAO Cost Estimating and Assessment Guide March 2009: http://www.gao.gov/new.items/d093sp.pdf
- Interim Agency Information Security Policy: http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/ansp_interim_policy.pdf
- ISO Standard 27002: http://www.27000.org/iso-27002.htm
- Mobile Access Review Committee (MARC) Resource Page (URL add)
- PMBOK Project Management Institute Guide and Standards: http://www.pmi.org/PMBOK- Guide-and-Standards.aspx
- Privacy Policy: http://intranet.epa.gov/oei/imitpolicy/qic/pdfs/cio2151.0.pdf
- Procedures for Preparing and Publishing Privacy Act System of Records Notices: http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO2151-P-03.1.pdf
- Project Management Templates developed by Deloitte for EPA: http://intranet.epa.gov/otopintr/slcm
- Quality Policy: http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/2106-0.pdf
- Recommended Security Controls for Federal Information Systems and Organizations – NIST 800-53 Rev. 3: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3- final_updated-errata_05-01-2010.pdf
- Security Considerations in the System Development Life Cycle – NIST 800-64 Rev. 2: http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf

| System Life Cycle Management (SLCM) Procedure | | |
|---|---|---|
| Directive No.:<br>CIO 2121-P-03.0 | CIO Approval: 12/21/2017 | Transmittal No.: 12-004* |

## 9. DEFINITIONS

**Acquisition/Development Phase** – The SLCM phase where the system is acquired through the purchase of software and services to yield a system that satisfies the mission need established in the Definition Phase.

**Acquisition** – The step of the SLCM Acquisition/Development Phase for planning and acquiring the software, hardware, and services necessary to construct a planned system.

**Authorization to Operate** – The official management decision given by a senior Agency official to authorize operation of an information system and to explicitly accept the risk to Agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

**Business Case** – The official OMB CPIC submission that describes current business processes, possibly using activity and data models, associates current costs and performance with the models, and identifies gaps between current and desired outcomes. The Business Case develops and evaluates alternatives for improving the business based on readily available information.

**Business Justification** – Describes the compelling business rationale for developing or modernizing a system.

**Capital Planning and Investment Control (CPIC) Process** – The decision-making process for ensuring information technology investments. The process integrates strategic planning, budgeting, procurement, and the management of IT in support of Agency missions and business needs, as defined in the Clinger-Cohen Act (CCA) of 1996.

**Certification and Accreditation (C&A)** – The activities and processes required to maintain security of information systems, periodically review the security controls, and maintain the certification and authorization of the information system to operate, including activities involved in the security planning and security testing certification and authorization processes. The C&A phase of the security process is where the system staff (outlined in the security documentation) performs the day-to-day functions required to maintain an appropriate level of security to protect the system (ongoing while the system is in operation).

**Commercial Off-the-Shelf (COTS)** – A commercial product or information system available to the general public. COTS products contain pre-established functionality, although some degree of customization is possible.

**Concept Exploration** – The step of the SLCM Definition Phase that establishes the preliminary definitions of the business needs of the system sponsor. It explains the concept in sufficient detail for decision makers to determine whether and how to proceed.

**Control Gate** – Phase-driven “go/no-go” decision points with reviews SLCM activities to ensure compliance with appropriate OMB and EPA requirements. A system cannot proceed without a “go” decision by the appropriate senior manager for the specific control gate.

**Contingency Plan/COOP** – Contains emergency response procedures; backup arrangements, procedures, and responsibilities and post-disaster recovery procedures and responsibilities.

Contingency planning is essential to ensure that systems are able to recover from processing disruptions in the event of localized emergencies or large-scale disasters. It is an emergency response plan, developed in conjunction with application owners and maintained at the primary and backup computer installation to ensure that a reasonable continuity of support is provided if events occur that could prevent normal operations.

**Decision Papers –** The result of a phase review that culminates with a decision memo approving the system to progress to the next phase or halting system development until requirements are met.

**Definition Phase** – The SLC phase that result in a defined business justification for the system and a plan for implementation or acquisition. Upon completion of this phase, the project will have approval and funding to proceed.

**Design** – The step of the SLCM Acquisition/Development Phase where projects create detailed designs for system components, products, and interfaces and where initial test planning begins. The objective is to transform detailed, defined requirements into complete, detailed system specifications to guide the work of the Development step.

**Development** – The step of the SLCM Acquisition/Development Phase where production and assembly of all of the system components needed to complete the design and meet the mission needs takes place. The objective is to convert the work products of the Design step into a complete information system.

**Enterprise Architecture (EA)** – A strategic information asset base which defines business mission needs, the information content necessary to operate the business, the information technologies necessary to support business operations, and the transitional processes necessary for implementing new technologies in response to changing business mission needs. EA includes baseline architecture, target architecture, and an enterprise transition plan.

**Government Off-the-Shelf (GOTS)** – A product developed by or for a government agency that can be used by another agency with the product's pre-established functionality and little or no customization.

**Implementation Phase** – The SLC phase where activities involving moving a completed system (or system modifications) into the production environment and completing the necessary processes to allow users to access the system to perform the work identified in the mission take place.

**Information and Communication Technology.** Information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include, but are not limited to: computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; customer premises equipment; multifunction office machines; software; applications; Web sites; videos; and, electronic documents.

**Major Investment** – EPA uses OMB's definition of a Major investment, which can be found in the CPIC Procedures document. For EPA's OMB budget reporting, all Major IT investments must be reported in the Exhibit 53 and must submit a Capital Asset Plan and Business Case (Exhibit 300).

**Mobile App or Application** – any native or Web application (app) specifically designed to be accessed and utilized on a handheld mobile device, such as a cell phone, smart phone, tablet, or portable digital assistant (PDA).

**Native Mobile Apps** – Native apps can come preinstalled on a mobile device, such as a smart phone, but can also be downloaded from app stores and other websites. Native apps can be programmed to leverage many smart phone capabilities, such as the camera and geo-location.

**Mobile Web Apps** - Mobile Web apps reside on a server and are accessed using a mobile browser. Mobile Web apps are distinct from mobile websites that only provide simple content.

Mobile Web apps use server-side or client-side processing (e.g. JavaScript) to provide a level of interactivity akin to many downloadable native apps.

**Mobile Websites** - A mobile website is a set of interconnected Web pages designed specifically to be accessed by mobile Web browsers.

**Non-Major IT Investment** – EPA uses the OMB's definition of a Non-Major investment, which can be found in CPIC Procedures. For EPA's OMB budget reporting, all Non-Major IT investments must be reported in the Exhibit 53.

**Pre-Definition Phase -** The Pre-Definition Phase is the first phase in the life cycle and is when business owners determine if an IT System or Solution is needed to fulfill a business need and/or performance gap.

**Project Level Reviews** – Reviews conducted at the project level to determine system readiness to proceed to the next phase of the IT life cycle. Key project stakeholders review and agree that the system under development is the system that needs to be built and that it is being built correctly. The System Manager and System Owner sign off on the completed review.

**Operations and Maintenance (O&M) Phase** – The SLCM phase where users have a working system to support the mission need. More than half of a typical system's life cycle costs are attributable to O&M, making the management of this phase of equal importance to the other phases that deliver the functionality. During this time, the Project Manager maintains schedules and periodically conducts reviews to ensure the health of the system and to validate the suitability of the system for meeting the requirements.

**Quality Management** – Ensures the quantity and quality of the data's intended use. Under the EPA Quality System, Agency organizations develop and implement supporting quality systems. Similar specifications may also apply to contractors, grantees, and other recipients of financial assistance from EPA.

**Security Testing and Evaluation (ST&E)** – An examination or analysis of the protective measures placed on fully integrated and operational information system. ST&E's objectives are to uncover design, implementation, and operational flaws that could allow the violation of security policy; determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy; and assess the degree of consistency between the system documentation and its implementation. The scope of an ST&E Plan typically addresses computer security, communications security, emanations security, physical security, personnel security, administrative security, and operations security.

**Segment Architecture** - The Segment Architecture is a set of documents that describe the baseline and target states of a Segment, as well as the transition between those states. The Segment Architecture is developed according to the goals and scope defined in the Segment Architecture Charter. The target recommendations that result from a Segment Architecture may lead to either the development of new IT systems and processes or the modification of existing systems and processes.

**Small Desktop Applications** – End-user programs or applications that reside solely on a desktop or laptop which, while they may interconnect with other applications, do not control, integrate, or manage components of a system.

**Solution Architecture** – A blueprint of an information management system, including its business processes, data classes, security controls, application interfaces, and technologies.

**System (Information System)** – NIST defines an information system as "A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" (NIST SP 800-18 Rev. 1). Federal guidance gives agencies flexibility in constituting an information system and system managers must establish system boundaries to define the information resources allocated to the system. A single system may consist of several subsystems (*a component of a system that performs specific functions*). These subsystems fall under the governance of the overall system and should be included in the system documentation, but they do not require separate documentation. A system or subsystem may include information resources e.g. applications, web pages, databases, or spreadsheets. On their own these resources are not considered an information system, but once combined with other resources to perform a specific function or process it becomes a system or subsystem.

**System Planning**– The step of the SLCM Definition Phase where creation of the necessary management structure to properly manage and control the system occurs and the Project Manager and System Manager create many of the plans essential to the success of the project. Reviewing and updating the plans takes place throughout the remaining SDLC phases. The System Manager further develops the plan for how the business will operate after implementation of the approved system occurs and an assessment of how the implemented system will impact employee and customer privacy takes place.

**System Lifecycle (SLC) –** EPA's System Lifecycle is the Agency's approach and practices in the definition, acquisition, development, implementation, operations and

maintenance, and termination of EPA information technology (IT) systems and applications. System owners and project managers must maintain required documentation for each phase, step, and activity during the lifecycle of an IT system or application. Each system must fit within the overarching Enterprise Architecture (EA) of the Agency, and thus the System Lifecycle includes control gates where management can review and approve EA, security, and system requirements before the system may proceed to the next phase of its lifecycle.

**Target Architecture** – A portrayal of the future enterprise. A high-level master blueprint describing the optimal state of the Agency, or an individual segment, in terms of strategic goals, business practices, data assets, IT services and technical infrastructure. Commonly referred to as the "to-be" architecture.

**Termination Phase** – The phase of the SLCM where system shutdown occurs. The purpose is to arrange for the retirement of a system and orderly disposition of system assets. During this end-of-life cycle phase, a system designated as excess or obsolete is retired and closed down. The emphasis of this phase is to ensure the orderly packaging and archiving of data, procedures, and documentation to ensure the retention of all records and make it possible to reinstall the system and bring it back to operational status if necessary.

**Waiver** – Written justification for deviating from the SLCM process or for omitting sections or documents of the SLCM. The consideration of waivers depends on the requirements of the system and the needs of the developing office. Waivers for major applications and general support systems and systems considered to be major investments in the CPIC process must receive concurrence from the System Owner and applicable IMO and approval from the Director of the Office of Environmental Information's Office of Technology Operations and Planning (OTOP). Waivers for any other applications and/or systems must receive concurrence from the System Owner and approval from the applicable IMO. Waivers should be documented as part of the Project Management Plan.

## 10. WAIVERS

Waivers to the requirements of this Procedure may be considered based on the requirements of the system and needs of the developing office. All waivers must be justified and documented (including all approvals and concurrences), by the information system Project Manager.

Any waiver requests must include a signed concurrence by the System Owner and the SIO or IMO (if delegated). While the CIO will approve SLCM Policy waivers, the Chief Technology Officer (CTO) will approve waivers from the SLCM Procedure or applicable standards.

## 11. MATERIAL SUPERSEDED

System Life Cycle Management Procedure; CIO Transmittal 07-003; Classification No.: 2121-P-01.0 (formerly 2111.5-P-01.0)

Interim Mobile Content and Concept Development Procedure; CIO Transmittal 11–00008; Classification No.: CIO 2121-P-02.0

| System Life Cycle Management (SLCM) Procedure | | |
|---|---|---|
| Directive No.:<br>CIO 2121-P-03.0 | CIO Approval: 12/21/2017 | Transmittal No.: 12-004* |

## 12. CONTACTS

For further information about this policy, please contact the Office of Environmental Information, Office of Digital Services & Technical Architecture, Technical Architecture & Planning Division.

***Steven Fine***
***Acting Chief Information Officer***
***U.S. Environmental Protection Agency***