INFORMATION DIRECTIVE
POLICY

System Life Cycle Management (SLCM) Policy		
Directive No.: CIO 2121.1	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) Policy

1. PURPOSE

The Environmental Protection Agency (EPA or Agency) strives to ensure that the process for managing the Agency's investments in Information Technology (IT) is consistent with federal statutes, regulations, and policies and supports EPA's System Life Cycle (SLC), Enterprise Architecture (EA), Capital Planning and Investment Control (CPIC), Quality and Information Security and Accessibility requirements. In order to maintain consistency with the mandates of the Clinger-Cohen Act of 1996, this document establishes the policy for assuring that IT resources are selected, developed and managed to achieve high value outcomes at acceptable costs. It also addresses the prescribed "select/control/evaluate" approach to managing IT investments.

The purpose of this policy is to establish a consistent framework across the Agency to ensure that EPA IT systems and applications are properly planned and managed, controllable, cost-effective and that they support the Agency's mission and business goals. This policy and its supporting documents provide EPA Offices with direction for tailoring and implementing System Life Cycle Management (SLCM) requirements to develop and manage effective and efficient IT solutions.

2. SCOPE

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.

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)

System Life Cycle Management (SLCM) Policy		
Directive No.: CIO 2121.1	CIO Approval: 12/21/2017	Transmittal No.: 12-004*

- Information Security Officers (ISOs)
- Information System Security Officers (ISSOs)
- System Sponsors
- System Owners
- System Managers
- Project Managers (PMs)

4. BACKGROUND

EPA invests in the acquisition, design, development, implementation, and maintenance of information systems vital to Agency programs and the administrative functions that support the protection of human health and safeguarding the natural environment. The need for safe, secure, reliable and accessible IT solutions is heightened by the increasing dependence on computer systems and technology to provide services, develop products, administer daily activities, and perform management functions.

There is also an increased importance on ensuring privacy, security and accessibility when developing information systems. It is necessary to establish uniform privacy and security practices, and to develop acceptable implementation strategies for these practices.

This policy meets EPA's need for a systematic and uniform methodology for information systems development and management. The policy will ensure that EPA information systems meet mission objectives; are compliant with the current and planned Enterprise Architecture (EA); are easy to maintain and cost-effective to enhance. Sound methodology promotes reliable, valid, and repeatable development and management practices.

5. AUTHORITY

- Chief Financial Officers Act of 1990
- Clinger-Cohen Act of 1996
- Federal Information Security Management Act (FISMA) of 2002
- Government Paperwork Elimination Act of 1998
- Paperwork Reduction Act of 1995
- Privacy Act of 1974, as amended
- Government Performance and Results Act of 1993
- OMB Circular No. A-11
- OMB Circular No. A-127 – Financial Management Systems
- OMB Circular No. A-130 – Management of Federal Information Resources
- Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794 (d)), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998.
- Information and Communication Technology (ICT) Final Standards and Guidelines (36 CFR Part 1193 and 1194, January 18, 2017).
- Section 255 (of the Communications Act of 1934, as amended by the Telecommunications Act of 1996 – 36 C.F.R. Part 1193

System Life Cycle Management (SLCM) Policy		
Directive No.: CIO 2121.1	CIO Approval: 12/21/2017	Transmittal No.: 12-004*

6. POLICY

A System Life Cycle (SLC) at EPA consists of six phases: Pre-Definition, Definition, Acquisition/Development, Implementation, Operations and Maintenance, and Termination. Detailed information on the steps required for each phase is defined in the supporting SLCM Procedure document.

- All EPA information systems must have a designated System Sponsor, System Owner, System Manager, and Project Manager to support the SLCM process.
- Documentation and/or artifacts required for each SLCM phase must be created and then updated throughout the system's life cycle. The life cycle phases needed for an information system must be identified, planned for, and executed based on documented business requirements and federal IT security requirements.
- The order of implementing SLCM phases and the level of detail required to complete them, can vary on a system-by-system basis. This Policy supports multiple development methodologies including agile and iterative development. Tailoring of the SLCM process must be documented as defined in the SLCM Procedure.
- Information security considerations, activities, and documentation are performed at each phase of the SLC in accordance with Agency policies and applicable federal statutes, regulations, National Institute of Standards and Technology (NIST) guidance, and other applicable federal or Agency requirements.
- Although all phases must be completed and documented, they do not need to occur in a linear fashion and non-linear development does not require a waiver.
- SLCM requires documentation. Documenting each major step or element will help ensure sound system life cycle management, Enterprise Architecture compliance, and alignment with IT investment management processes. The Project Manager and System Manager ensure that the required documentation is updated as appropriate throughout the system's life cycle.
- System Owners and System Managers must review and approve the system's tailoring decisions. The Project Manager must document the tailoring reviews and approvals in the system's decision documents.
- Advancement from one SLCM phase to the next requires Enterprise Architecture, IT investment management, or information security reviews. These reviews are designated by Agency-level control gates and System Owners and System Managers must ensure they take place. When a control gate review is required, System Managers must not advance a system without documented, written approval resulting from that review. Additionally, management must ensure that all calendar-driven checkpoints and phase-level reviews are conducted. The timing and method of the reviews will vary based on the tailoring plan of the specific system.
- Section 508 of the Rehabilitation Act as amended (29 U.S.C. § 794d) mandates the development, procurement, maintenance and use of Information and Communication

Technology (ICT) is accessible to people with disabilities. Each federal agency must ensure – unless it would impose an undue burden to do so – its ICT allows individuals with disabilities, both federal employees and members of the public, access to and use of information and data comparable to that available for people without disabilities. Incorporation of Section 508 requirements into system lifecycle activities including enterprise architecture, design, development, testing, deployment and ongoing maintenance activities will ensure the accessibility of ICT.

7. ROLES AND RESPONSIBILITIES

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

- Approving the SLCM Policy and Procedure
- Ensuring Agency compliance with the SLCM Policy by providing guidance and tools to senior managers for program oversight
- Deciding on waiver requests to requirements of 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 and Enterprise Transition Planning in conjunction with the SLCM Policy and Procedure
- Certifying and providing guidance for compliance of solution architectures during EA reviews.

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
- Approves a project to continue through control gates (this may be delegated for smaller systems)
- Reviewing, concurring, advising and/or submitting waiver requests to the SLCM Policy and Procedure, as applicable

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 SLCM security documentation, 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

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, as applicable

System Owners are responsible for:

- Monitoring compliance to the SLCM Policy and Procedure and approving tailoring plans
- Appointing Project Managers and System Managers
- Coordinating SLCM development activities with those of the EA, IT Investment Management, and Information Security processes
- Serving as the information owner of the system
- Ensuring compliance to Section 508 requirements during the SLCM
- Concurring on waiver requests from the SLCM Policy and/or Procedure, as applicable
- Approving completed Control Gate and Project Level Reviews

System Managers are responsible for:

- Providing day-to-day management of the system life cycle process and products within their programs

- Ensuring that their systems advance through the SLCM phases and activities
- Creating an SLCM Tailoring plan and submitting it for approval by the System Owner
- Recommending and preparing written justification for waiver requests 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 its life cycle
- Incorporating the SLCM artifacts and work products in the system project schedule
- Assigning resources on the system project team to complete SLCM artifacts

Privacy Act Officer is responsible for:

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

8. RELATED INFORMATION

DOCUMENTS

- 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
- 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
- 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 Records Management Policy: http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO- 2155.1_2.pdf
- FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- GAO Cost Estimating and Assessment Guide March 2009: http://www.gao.gov/new.items/d093sp.pdf
- Interim Agency Network Security Policy:

http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/ansp_interim_policy.pdf

- Mobile Access Review Committee (MARC) Resource Page (URL add)
- 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
- 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

PROCEDURES, STANDARDS AND GUIDANCE

- System Life Cycle Management Procedure - http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO 2121-P-03.0.pdf
- System Life Cycle Management Documents Guidance - http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO 2121-G-01.0.pdf

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.

Application – The information resources (usually software) used to satisfy a specific set of user requirements (OMB A-130, Appendix III). In particular, an application usually refers to the software component of a system.

Artifacts – Work products created throughout the life cycle documenting activities, decisions, and requirements. Artifacts may be paper documents or electronic files and are based on best practices and guidance for project and IT management.

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.

Checkpoint – A specific calendar-driven point during the SLC when the System Owner assesses the progress of the SLCM process to ensure that the activities associated with this process coordinate with and support the CPIC, EA, and IT Security requirements.

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.

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.

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.

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.

Information Technology (IT) – Applied computer systems, both hardware and software, and often including networking and telecommunications, usually in the context of a business or other enterprise.

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.

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 O&M the System Manager maintains schedules and periodically conducts reviews to ensure the health of the system and to validate the suitability of the system for meeting SLCM requirements.

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.

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.

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 requirements of the SLCM Policy. The consideration of waivers depends on the requirements of the system and the needs of the developing office. SLCM Policy Waivers must receive concurrence from the System Owner and applicable SIO/IMO and receive approval from the CIO.

System Life Cycle Management (SLCM) Policy		
Directive No.: CIO 2121.1	CIO Approval: 12/21/2017	Transmittal No.: 12-004*

10. WAIVERS

Waivers to the requirements of this Policy 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 System Manager.

Any waiver requests must include a signed concurrence by the System Owner and the SIO or IMO (if delegated). 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 Policy, CIO Policy Transmittal 06-009, Classification No.: CIO 2121 (formerly 2100.5)

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