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

System Life Cycle Management Policy

1. PURPOSE

The purpose of this policy is to ensure that the Environmental Protection Agency (EPA or Agency) provides a framework to manage the Agency's investments in Information Technology (IT) that is consistent with federal statutes, regulations and policies in support of the Agency's mission and business goals. The Clinger-Cohen Act of 1996 and the Federal Information Technology Acquisition Reform Act (FITARA) of 2014 establish Chief Information Officer (CIO) authority to provide IT policy, set management activities, oversee budget accountability and promote transparency for IT investments. There is also an increased importance for federal agencies to share information systems and IT solutions while ensuring privacy, security and accessibility when developing IT. EPA promotes the re-use and collaborative development of IT solutions across the Agency. This policy provides a consistent methodology and governance for information system development and management. Lastly, this policy will strengthen the relationship between the CIO and program offices that will support accountability and transparency in managing EPA's IT resources.

2. SCOPE

The Application Review Process cited in the Pre-Definition Phase of the SLCM applies to all new systems or applications that meet the criteria maintained on EPA's Application Review Process (ARP) site. This holds even if the application is not of sufficient size or scope to require strict compliance with the rest of this policy.

Beyond compliance with the Application Review Process, this policy applies to:

- EPA programs, acquisitions and solutions with an IT component (including interagency or government-wide initiatives)
- IT systems, applications, projects and general support systems (GSS)
- Custom-developed, commercial off-the-shelf (COTS), or government off-the-shelf (GOTS) information technology and Software as a Service (SaaS) applications
- Applications, solutions or systems developed on behalf of EPA by other federal agencies or contractors irrespective of where the IT systems are hosted; including cloud-based solutions

Small internal facing applications using Agency-provided COTS/SaaS services where no custom code is being generated and there is no additional procurement outside of Agency provided services, are excluded from the requirements of this policy – with the exception of complying with the Application Review Process.

3. AUDIENCE

The audience for the policy includes 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)
- Chief Architect (CA)
- Information Management Officers (IMOs)
- Information Security Officers (ISOs)
- Information System Security Officers (ISSOs)
- System Sponsors
- System Owners
- System Managers
- Project Managers (PMs)
- Senior Information Technology Leaders (SITLs)

4. BACKGROUND

The Clinger Cohen Act of 1996 and the Federal Information and Technology Acquisition Act (FITARA) of 2014 provide authority to Federal CIOs to manage IT investments in their agencies. EPA invests in the acquisition, design, development, implementation and maintenance of information systems and solutions that are vital to the Agency's mission to protect human health and the 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.

5. AUTHORITY

- Chief Financial Officers Act of 1990 H.R.5687 - 101st Congress (1989-1990): Chief Financial Officers Act of 1990 | Congress.gov | Library of Congress
- Clinger-Cohen Act of 1996 https://www.govinfo.gov/content/pkg/USCODE-2011-title40/pdf/USCODE-2011-title40-subtitleIII.pdf
- Interim E-Enterprise for the Environment Digital Strategy https://e-enterprisefortheenvironment.net/wp-content/uploads/2019/08/Interim-E-Enterprise-Digital-Strategy-V-2.0.pdf
- Federal Information Security Modernization Act (FISMA) of 2014 https://www.congress.gov/bill/113th-congress/senate-bill/2521/text
- Federal Information Technology Acquisition Reform Act (FITARA) of 2014 https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf#page=148%5D
- Government Paperwork Elimination Act of 1998 https://www.congress.gov/bill/106th-congress/house-bill/439
- Office of Management and Budget (OMB) Memorandum M-16-21, Federal Source Code Policy

https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

- Paperwork Reduction Act of 1995 https://www.govinfo.gov/content/pkg/PLAW-104publ13/html/PLAW-104publ13.htm
- Privacy Act of 1974, as amended https://www.justice.gov/opcl/privacy-act-1974
- Government Performance and Results Act of 1993 https://www.congress.gov/bill/103rd-congress/senate-bill/00020
- Digital Government Strategy, 2012 https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf
- Federal Cloud Computing Strategy, 2019 https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf
- Section 508, Rehabilitation Act, 1973 https://www.govinfo.gov/content/pkg/USCODE-2011-title29/html/USCODE-2011-title29-chap16-subchapV-sec794d.htm
- Section 255, Communications Act, 1996 https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-telecommunications-act-guidelines

6. POLICY

System Life Cycle Management (SLCM) 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.

- EPA information systems must have a designated System Sponsor, System Owner, System Manager and Project Manager to support the SLCM process.
- EPA information systems acquisitions over $1M/year must be reviewed and approved by the CIO.
- EPA information systems acquisitions less than $1M/year must be reviewed and approved by the Chief Technology Officer (CTO).
- EPA information systems must be designed, developed and implemented by utilizing an enterprise shared solutions (ESS) approach when practicable.
- EPA must share, document and manage new custom-developed code created by or on behalf of the Agency, or procured for broad reuse across the federal government.
- EPA information systems (new, modernizations and terminations) must be vetted within the control gate phases to ensure alignment to EPA's enterprise architecture (EA), eliminate redundancies, leverage ESS, and ensure cost effectiveness.
- 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, section 508 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 development. Tailoring of the SLCM process must be documented as defined in the SLCM Procedure.

- Information security considerations, activities, and documentation are performed during each phase of the system life cycle 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.
- SLCM Phases 1 and 2 must be performed regardless of the development methodology. Subsequent SLCM phases must be completed and documented, but they do not need to occur in a linear fashion.
- Project Managers and System Managers must 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 and information security reviews. These reviews are designated by Agency-level control gates. System Owners and System Managers must ensure that control gate reviews take place when they are required, System Managers must not advance an IT system, solution, application or program without documented SIO approval resulting from that review.
- Proposals for new IT solutions, system modernizations and terminations must be presented to the CIO SAC during control gates 2 and 5 to manage enterprise-wide impacts. Additionally, System Managers 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 IT project.
- Section 508 of the Rehabilitation Act as amended (29 U.S.C. § 794d) mandates that 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 life cycle 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) is responsible for:

- Approving the SLCM Policy and Procedure
- Reviewing and approving EPA information systems/investments acquisitions that are $1M or greater or that meet other needs for CIO attention
- Resolving disputes identified during the Application Review Process (ARP)
- Ensuring custom-developed code that EPA develops or procures is shared for broad

use across the federal government, subject to limited exceptions
- Ensuring Agency compliance with the SLCM Policy by providing guidance and tools to senior managers for program oversight
- Deciding on requests to waive 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, 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
- Reviewing and approving EPA information systems acquisitions less than $1M/year
- Promoting adoption of Agile development
- Promoting the adoption of EPA enterprise digital and shared services strategies

Chief Acquisition Officer (CAO) is responsible for:

- Ensures Contracting Officers (CO) and Contracting Officer's Representatives (COR) obtain the appropriate government data rights to custom-developed code, including, at a minimum, data right clauses, rights to distribute source code, rights to reuse and rights to modify code in order to share custom-developed code EPA develops or procures for broad reuse across the federal government, subject to limited exceptions.

Chief Information Security Officer (CISO) is responsible for:

- Providing oversight to the Agency's security assessment and authorization process and status
- Reviewing authorization packages and making authority to operate (ATO) decision recommendations to the CIO

Chief Information Officer – Senior Advisory Committee (CIO SAC) is responsible for:

- Reviewing and recommending enterprise IT strategic direction and criteria for making IT investment decisions
- Advising on IT annual budget as it relates to IT strategic direction
- Advising on requests for new IT solutions, system modernizations and terminations

Office of Digital Services and Technical Architecture is responsible for:

- Maintaining SLCM Directives
- Monitoring compliance with the SLCM through EA, IT Investment Portfolio Reviews and security processes

Chief Architect is responsible for:

- Leading the development and implementation of EPA's Enterprise Architecture and Digital Strategy
- Certifying and providing guidance for compliance of solution architectures during EA

reviews

Director of the Office of Acquisition Solutions (OAS) 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 members of the Agency IT Governance body of major SLCM issues within their offices
- Ensuring compliance with the SLCM Policy and Procedure for systems within their offices
- Ensuring that the IT used and managed by their organization supports its business needs and mission and helps to achieve strategic goals
- Ensuring EA compliance of solution architectures
- Approving a project to continue through control gates (this may be delegated for smaller systems)
- Reviewing, concurring on, advising on and/or submitting requests to waive SLCM Policy and Procedure requirements, 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 requests to waive SLCM Procedure requirements, as applicable
- Reviewing, approving and supporting the development of accessibility documentation, as appropriate
- Reviewing requests for exceptions to sharing custom-developed code.

Information Security Officers (ISOs) are responsible for:

- Reviewing and supporting the development of SLCM security documentation, as appropriate
- Assigning 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 with Section 508 requirements during the SLCM process
- Ensuring systems managers appropriately search for and implement ESS to address systems requirements
- Concurring on requests to waive SLCM Policy and/or Procedure requirements, as applicable
- Approving completed Control Gate and Project Level Reviews
- Sharing custom IT solutions developed within their offices with the Agency Enterprise Code Repository

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
- Searching service catalogs and resources and implementing applicable ESS to meet systems requirements
- 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

Senior Information Technology Leaders (SITLs) 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 from the system project team to complete SLCM artifacts
- Applying open development practices when developing custom-developed code
- Sharing custom IT solutions developed within their offices with the Agency Enterprise Code Repository

Code Repository Owners are responsible for:

- Managing a code repository using Agency authorized services.
- Selecting the appropriate open source license for broad reuse across the federal government, subject to limited exceptions
- Selecting the appropriate rights license to provide the government's rights to share custom-developed code with other agencies where EPA is not seeking or able to obtain the rights to publicly release the code

- Releasing public code that leverages existing communities in order to:
  (1) foster solutions for shared challenges,
  (2) improve the ability of the OSS community to provide feedback on, and make contributions to, the source code, and
  (3) encourage federal employees and contractors to participate in the OSS community by making contributions to existing OSS projects.
- Fostering open development practices when developing custom-developed code
- Sharing custom IT solutions developed within their offices with the Agency Enterprise Code Repository

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

- Interim Capital Planning and Investment Control Program Policy: https://www.epa.gov/sites/production/files/2021-01/documents/interim_capital_planning_and_investment_control_program_policy.pdf
- Interim Capital Planning and Investment Control Procedures: https://www.epa.gov/sites/production/files/2021-01/documents/interim_capital_planning_and_investment_control_procedures.pdf
- System Life Cycle Management Procedure: https://www.epa.gov/sites/production/files/2021-02/documents/system_life_cycle_mangaement_procedure.pdf
- Section 508: Accessible Electronic and Information Technology (EIT): https://www.epa.gov/sites/production/files/2015-03/documents/2130.1.pdf
- Accessible Electronic and Information Technology Standards, Procedures, and Guidance: https://www.epa.gov/sites/production/files/2013-11/documents/2130psg010.pdf
- Data Exchange Procedure: https://www.epa.gov/sites/production/files/2018-03/documents/data_exchange_procedure.pdf
- Data Standards Policy: https://www.epa.gov/sites/production/files/2013-11/documents/21330.pdf
- Enterprise Architecture Procedure: https://www.epa.gov/sites/production/files/2013-11/documents/cio-2122.1.pdf
- EPA Acquisition Regulation (EPAAR): https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title48/48cfrv6_02.tpl
- Interim Records Management Policy: https://www.epa.gov/sites/production/files/2018-09/documents/interim-records-mgmt-policy-20180822.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

- Information Security Policy: https://www.epa.gov/sites/production/files/2019-09/documents/information_security_policy_20190820_508_vwn.pdf
- Privacy Policy: https://www.epa.gov/sites/production/files/2015-09/documents/2151.1.pdf
- Procedures for Preparing and Publishing Privacy Act Systems of Records Notices: https://www.epa.gov/sites/production/files/2015-09/documents/2151.1.pdf
- Recommended Security Controls for Federal Information Systems and Organizations – NIST 800-53 Rev.4: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
- OMB Memorandum M-19-18, Federal Data Strategy: https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf
- OMB Memorandum M-19-21, Transition to Electronic Records: https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-21.pdf
- OMB Memorandum M-19-16, Centralized Mission Support Capabilities for the Federal Government: https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-16.pdf
- OMB Memorandum, Strategic Plan for Improving Management of Section 508 of the Rehabilitation Act: https://obamawhitehouse.archives.gov/sites/default/files/omb/procurement/memo/strategic-plan-508-compliance.pdf
- Information and Communication Technology (ICT) Final Standards and Guidelines: https://obamawhitehouse.archives.gov/sites/default/files/omb/procurement/memo/strategic-plan-508-compliance.pdf
- CIO Memorandum: EPA's Approach to Implementing Shared Services

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 resource or solution 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 system life cycle 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 of 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.

Custom-Developed Code – Code that is first produced in the performance of a federal contract or is otherwise fully funded by the federal government. It includes code, or segregable portions of code, for which the government could obtain unlimited rights under Federal Acquisition Regulations (FAR) Pt. 27 and relevant agency FAR Supplements. Custom-developed code also includes code developed by agency employees as part of their official duties. For the purposes of this policy, custom-developed code may include, but is not limited to, code written for software projects, modules, plugins, scripts, middleware and application programming interfaces (APIs); it does not, however, include code that is truly exploratory or disposable in nature, such as that written by a developer experimenting with a new language or library.

Definition Phase – The SLCM phase that results 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.

Enterprise Shared IT Service (ESS) – A centrally provided IT service with defined service levels, costs, and methods of integration that is designed to be used or consumed by any part of the enterprise with a business requirement or need. EPA's centrally provided shared technical infrastructure services include email and collaboration tools, data center hosting, and network management. EPA shared applications services include access to payroll and other enterprise applications. EPA plans to expand its SS portfolio into software delivery services and shared data services in the future.

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 SLCM phase that involves 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.

Information and Communication Technology (ICT) – 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, websites 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 IT Investment – EPA uses OMB's definition of a Major IT Investment, which can be found in the CPIC Procedures document. For OMB budget reporting, EPA must report all Major IT Investments in the Exhibit 53 and 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 OMB budget reporting, EPA must report all Non-Major IT investments in the Exhibit 53.

Pre-Definition Phase – The first phase in the life cycle where 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 approve the completed review.

Open Source Software (OSS) – Software that can be accessed, used, modified and shared by anyone. OSS is often distributed under licenses that comply with the definition of "Open Source" provided by the Open Source Initiative4 and/or that meet the definition of "Free Software" provided by the Free Software Foundation.

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 they become a system or subsystem.

Termination Phase – The phase of the SLCM process 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.

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 will approve waivers to the SLCM Procedure or applicable standards.

11. MATERIAL SUPERSEDED

System Life Cycle Management Policy, CIO Policy Transmittal 12-004, Classification No.: CIO 2121.1.

12. CONTACTS

For further information on this policy, contact your Information Management Officer. You may also contact the Office of Mission Support, Environmental Information, Office of Digital Services & Technical Architecture.

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2021.02.26 15:21:19 -05'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency