

CENTERS FOR MEDICARE & MEDICAID SERVICES
Office of Enterprise Information (OEI)
7500 Security Boulevard
Baltimore, Maryland 21244



CMS Chief Information Officer (CIO) Policy Framework

Issued:	09/15/2015
Last Revised:	12/21/2015
Document Control #:	CMS-CIO-POL-1000.00

Record of Changes

Version	Date	Author/Owner	Description of Change
1.0	09/15/2015	OEI/DPPIG	Baseline version of policy.
1.01	12/21/2015	OEI/DPPIG	Minor errors corrected.

Effective Date / Approval

This policy becomes effective on the date that CMS' Chief Information Officer (CIO) signs it and remains in effect until it is rescinded, modified or superseded by another policy.

This policy must not be implemented in any recognized bargaining unit until the union has been provided notice of the proposed changes and given an opportunity to fully exercise its representational rights.

Signature: _____ /s/ _____ Date of Issuance: 09/15/2015
David Nelson
Deputy Chief Operating Officer,
Chief Information Officer

Policy Owner's Review Certification

This document must be reviewed in accordance with the established review schedule located on the [CMS website](#).

Signature: _____ Date of Annual Review: _____
[Reviewer's Name]
[Reviewer's Organization]

Table of Contents

1	Policy Statement.....	1
2	Background.....	1
3	Scope	2
4	CIO Policy Documentation Hierarchy at CMS.....	2
4.1	Policy	2
4.2	CIO Directive.....	3
4.3	CMS Technical Standards.....	3
4.4	Guidelines and Best Practices	3
4.5	CIO Procedures.....	4
5	Policy.....	4
5.1	General Principles	4
5.2	Emergency Policies	5
5.3	Policy Format, Content, and Style	5
5.4	Annual Document Review	5
5.4.1	Policy Revocation	6
6	Stakeholder Involvement.....	6
6.1	Policy Development Workgroups	6
7	Publication and Communication Methods.....	7
8	Roles and Responsibilities.....	7
8.1	Chief Information Officer (CIO).....	7
8.2	Deputy CIO	8
8.3	Chief Technology Officer (CTO).....	8
8.4	Management Officials	8
8.5	Division of Policy, Program Integration, & Governance, Division Director	8
8.6	CMS CIO Policy Officer	8
8.7	Policy Staff.....	9
8.8	Policy Owner	9
8.9	Critical Partners	9
8.10	Office of Technology Solutions and Office of Enterprise Information	10
8.11	CMS Employees and Users of CMS IT Resources.....	10

9 Metrics.....11

10 Information and Assistance.....11

11 Applicable Laws/Guidance.....11

12 Reference Documents.....11

13 Glossary.....12

Appendix 1: CIO Policy Life Cycle.....15

Appendix 2: CIO Policy Framework Structure20

1 Policy Statement

The Centers for Medicare & Medicaid Services (CMS) Chief Information Officer (CIO) Policy Framework governs the development, review, approval, maintenance, and revocation of agency-level CIO policy documents written by CMS or on behalf of CMS. CIO policy documents include policies, technical standards, directives, guidelines, and procedures that encompass topics related to information technology (IT) and information security and privacy.

This policy serves to:

- Establish standards for the development and clearance of CIO policies
- Establish CIO policy standards of content, uniform format, and style
- Establish requirements for maintaining the administrative records documenting the development and issuance of all CIO policies
- Require periodic reviews of existing CIO policies to determine the need for revision and/or improvement
- Describe the revocation process for applicable CIO policies

The CMS CIO Policy Framework also formally establishes the *CIO Policy Vetting and Clearance Process* for CIO policy review and approval. *See Appendix 1: CIO Policy Life Cycle.*

Finally, this framework specifies:

- A structure and criteria for what should be categorized as a CIO policy, guideline, directive, technical standard, or procedure
- Processes for CIO Policy Framework life cycle activities
- Ongoing roles and responsibilities associated with CIO policy development and maintenance

This CIO policy is a first issuance.

2 Background

An important foundational element in support of the CMS IT governance program involves establishing an agency-level CIO policy function. The CIO policy function resides with the Office of Enterprise Information with delegated responsibilities for policy development, coordination, education, and maintenance. The responsibilities associated with the CMS CIO Policy Framework include:

- Coordination of CIO policy and underlying development, dissemination, education, and maintenance
- Review and analysis of existing CIO policies for continued applicability and effectiveness
- Interpretation of current policy related to specific issues, situations and incidents

CIO policies articulate CMS' vision, strategy, and core values as they relate to the management and use of information and information technology resources, while supporting CMS' mission - *as an effective steward of public funds, CMS is committed to strengthening and modernizing the nation's health care system to provide access to high quality care and improved health at lower cost.*

Further, CIO policies ensure compliance with applicable laws and regulations and with all other authoritative sources such as mandates, directives, executive orders, and HHS policy. Finally, CIO policies help to promote operational efficiency and manage risk to the agency by specifying requirements and standards for the consistent management of IT resources across CMS.

3 Scope

All facets of CIO policy development, review, maintenance, and revocation, as stated in this policy, are in effect and apply to all agency-level CIO policies. It is important to note that IT policies and related documents developed specifically for the operations of individual Centers, Offices, Groups, or Divisions (i.e., developed for a limited audience) are out of scope.

This policy applies to all CMS employees and organizations conducting business for and on behalf of CMS through contractual relationships when managing and using CMS IT resources. This policy does not supersede any other applicable law or higher level agency directive, or existing labor management agreement in effect as of the effective date of this policy.

4 CIO Policy Documentation Hierarchy at CMS

The CMS CIO Policy Framework uses agency-level policies, directives, guidelines, procedures, and technical standards to convey IT Governance.

Categories of CIO documents are described below. See *Appendix 2: CIO Policy Framework Structure* for additional information about these categories.

4.1 Policy

A policy is a guiding principle, direction, or expectation typically established by CMS senior management to influence and determine decisions. A CIO Policy is usually predicated on oversight requirements. Typical characteristics: (1) Include clear, concise and simple language and comply with the Plain Language Act of 2010; (2) Contain "must" statements; (3) Address what the rule is rather than how to implement it; (4) Is readily available to all affected parties; (5) Results in punitive actions for failure to comply.

CMS CIO policies are mandatory. All new or substantially revised CIO policies require substantial agency-wide vetting and clearance by the CIO. Once complete, these policies are submitted for version control and posted on the public-facing CMS website. *Note: Policies containing sensitive information are subject to restricted distribution and may not be posted on the CMS website.*

Examples of CIO Policies:

- CMS Information System Security and Privacy Policy (CISSPP)

- Policy for Information Technology (CIO) Investment Management & Governance
- Policy for Section 508 Compliance

4.2 CIO Directive

A CIO Directive allows the CIO to respond to identified gaps in CMS policy and instruction. Directives are used to issue direction on policy-level issues where current direction does not exist. CIO Directives may also serve as a stop-gap to provide immediate guidance while a policy is being developed/updated, cleared, and approved. CIO Directives may require action or may be for informational purposes to help clarify existing policy.

Examples of CIO Directives:

- CIO Directive 13-01: Policy for Monitoring Use of CMS IT Resources
- CIO Directive 14-04: CMS Encryption of Sensitive Information in Email

4.3 CMS Technical Standards

For the purposes of this policy, a technical standard refers to one or more related technical specifications that have been internally developed, sanctioned, and mandated for use by CMS. CMS' technical standards are documented in the form of the CMS Technical Reference Architecture (TRA) and Supplements, and information security standards. The CMS TRA specifies standards for compliance with CMS' Enterprise Architecture, CIO policies, and the CMS Acceptable Risk Safeguards (ARS). CMS technical standards are enforced based on CMS-defined conformance criteria.

Examples of Technical Standards:

- Data Warehousing
- Enterprise File Transfer
- Standards portion of the Risk Management Handbook

4.4 Guidelines and Best Practices

Guidelines provide guidance and best practices relative to a particular topic. They may accompany, interpret, or provide guidance for implementing CIO policies, or may provide guidance to various CMS IT Life Cycle activities. Guidelines are recommended best practices but are not required to be in compliance with policy. A guideline aims to streamline particular processes according to a set routine or sound practice. By definition, following a guideline is never mandatory. Guidelines are not binding and are not enforced. Some CMS IT guidelines are referred to as "Practices Guides".

A best practice is a technique, method, process, activity, incentive, or reward that is believed to be one of the most effective approaches for delivering a particular outcome when applied to a particular condition or circumstance. The idea is that with proper processes, checks, and testing, a desired outcome can be delivered with fewer problems and unforeseen complications. Best practices can also be defined as the most efficient (least amount of effort) and effective (best

results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of people. A best practice can be adopted as a guideline.

Examples:

- Lessons Learned Guidance

4.5 CIO Procedures

CIO procedures consist of step by step instructions to assist workers in implementing policies, standards, and guidelines. Procedures document “how to” accomplish specific IT tasks or use IT services. These procedures may apply at the agency level or they may be localized to reflect the practices or requirements of a specific CMS office, center, group, division, or workgroup.

Examples:

- Procedure portions of the Risk Management Handbook

5 Policy

5.1 General Principles

The CIO Policy Framework employs the following principles:

- Policy work must be initiated when there is a compelling need for new or revised policy. Triggers may include new technologies, new laws or regulations, or operational or compliance needs that are not appropriately covered by existing policies or guidance.
- CIO policy development may be accomplished via individual workgroups convened to address specific topics. Each workgroup must include appropriate subject matter experts. For more information about policy development workgroups, refer to Section 6.1.
- The Division of Policy, Program Integration, & Governance (DPPIG) in the IT Investment Portfolio Management Group (IIPMG), Office of Enterprise Information (OEI) must provide a central coordination function to ensure consistency and to address policy dependencies.
- The policy development process must be transparent. All CIO policy writing, to the extent possible and practicable, must employ a collaborative effort during development and actively engage an even wider distribution during the policy’s review period, to gather a broad perspective of input. Input from stakeholders must be addressed and/or incorporated throughout the process as explained in *Appendix 1: CIO Policy Life Cycle*.
- All CIO policies must be maintained centrally and accessible to all interested stakeholders.
- All published CIO policies must be Section 508 compliant (i.e., fully accessible by disabled and non-disabled individuals).
- Policies and guidance must be implementable and sustainable. Impact risk analysis on both IT systems and end-users must be included in the policy planning and review processes.

- All CIO policies must be kept current through an organized system of change control. At a minimum, all CIO policies must be reviewed by the Policy Owner and, if necessary, updated on an annual basis or more frequently as significant changes are identified. *See Section 5.4 Annual Document Review* for annual policy review criteria and definition of “significant change” as it applies to this policy.
- Any employee or contractor may request consideration of new CIO policies or changes to existing policies.
- The policy development process must be flexible. Circumstances may necessitate the publishing of CIO Directives as a stop-gap to provide immediate guidance while a policy is being developed, vetted, and approved. In other cases, a policy may be established with detailed guidance to be provided at a later time.
- CMS offices/centers/groups/divisions must use this policy or may create a more restrictive policy, but not one that is less restrictive and/or less comprehensive.

5.2 Emergency Policies

In rare cases, such as the need for an emergency policy, the CIO may immediately issue a policy without prior stakeholder comment. The CIO may use this method on an exception basis when:

- The CIO deems it necessary to use sole discretion in determining the policy
- An urgent need exists for immediate notification of a new policy

Even in these rare situations, stakeholders always have the opportunity and responsibility to suggest and request changes. An emergency policy is not an interim policy for it carries the full weight of the CIO and is enforceable.

Please note that issuing a CIO Directive may be more appropriate than issuing an emergency policy when an urgent need exists for immediate notification of urgent information. CIO Directives often serve as a stop-gap to provide immediate guidance while a policy is being developed/updated, cleared, and approved.

5.3 Policy Format, Content, and Style

All CIO policies must conform to standard content, format, and style (font, headers & footers, margins, pagination, etc.), as specified in the *CIO Policy Template and Guide*.

5.4 Annual Document Review

Policy owners must review policies at least annually or more frequently as significant changes that impact the policy are identified. The term “significant change” refers to a change in federal legislation, mandates, directives, executive orders, and/or HHS policy that requires corresponding changes to be made to existing CMS policies.

The annual document review is a control mechanism to ensure CIO policies are reviewed by their respective owners on a regular basis to ensure accuracy and to identify areas of potential improvement. The *Annual Review Schedule* is located on the [CMS website](#).

During the annual document review, document owners must review the document(s) they own for at least the following:

- Inaccuracies
- Organizational changes affecting the document
- Process changes
- Metric changes
- New or now obsolete external references
- Internal reference document changes including titles
- Links, URLs, or email address changes
- Changes to databases or other data repositories used
- Changes to labor management agreements affecting the document
- Potential areas of improvement
- Incorporation of CIO Directives, as applicable. As CIO Directives are incorporated into policy, the directives are then revoked, as explained in Section 5.4.1 (Policy Revocation).

Refer to the *Master List* for ownership of each document.

5.4.1 Policy Revocation

As part of the maintenance and review process, policies, standards, procedures, and/or guidelines may be identified as out-of-date or no longer needed. They must be revoked via the same process by which they were approved and must be removed from externally accessible web sites upon revocation.

A CMS internal limited-access website (e.g., SharePoint) will be maintained where legacy versions of policies will be stored. This will ensure:

- compliance with NARA
- accessibility to previous versions policies should requirements reappear
- historical research

6 Stakeholder Involvement

CMS has a major role in CIO policy development and review with the intent of broad coordination and collaboration during CIO policy development and throughout the CIO policy review process.

Stakeholders must be engaged throughout the CIO policy development process—in both individual and group settings—to ensure that all appropriate perspectives are accounted for and incorporated as feasible in final versions of new or revised policies, standards, guidelines and procedures. DPPIG maintains a list of potential stakeholders to be involved at various stages in the CIO policy life cycle process.

6.1 Policy Development Workgroups

Specific individuals and groups must be identified during the planning and initiation phase of a given policy, standard, or guideline. Membership in policy development workgroups must vary based on the primary content of a policy being developed. The CMS CIO Policy Officer will serve ex officio and provide support to all working groups. In general, any CMS employee or CMS contractor must be able to provide comments on draft and interim policies, standards, and guidelines on the CMS CIO policy web site. Specific stakeholders may be identified and solicited to provide input and review, while others may be only in the “need to inform” category.

7 Publication and Communication Methods

To ensure timely access and operational effectiveness, finalized CIO policies and other CIO-related reference documents must be placed under version control by the CMS CIO Policy Officer and published on the [CMS CIO Resource Library website](#). The CMS CIO Resource Library must contain the currently-approved version of all CIO policies, CIO directives, technical standards, guidelines, and procedures. The documents on the CMS CIO Resource Library website must constitute the official electronic repository for agency-wide CIO documents for CMS. *Note: Policies containing sensitive information are subject to restricted distribution and may not be posted on the CMS website.*

Multiple communication methods will be employed to widely disseminate information about new or revised documents posted to the CMS CIO Resource Library website, including (but not limited to):

- CMS newsletters
- CMS broadcasts
- Digital signage
- Web feeds
- Listserv messages
- Announcements at TRB meetings
- e-mail distribution to CMS CORs and contractors, as appropriate

8 Roles and Responsibilities

The roles and responsibilities defined below represent the individuals or groups most directly involved in CMS CIO policy development.

Table 1: Summary of Roles and Responsibilities

Role	Responsibility and Authority
8.1 Chief Information Officer (CIO)	<p>The CIO has overall responsibility for IT policy and policy development at CMS, and final approval of new and revised policies and standards.</p> <p>The CIO is responsible for the following activities:</p>

Role	Responsibility and Authority
	<ul style="list-style-type: none"> • Reviewing and approving new policies as the final level of governance approval • Permitting employees to participate in policy development workgroups to help develop and review policies and to provide timely comments • Disseminating and implementing IT policy within CMS • When needed, developing and approving policies that are more restrictive than HHS policies but not ones that are less restrictive or less comprehensive • Training all employees on policies, as appropriate • Ensuring that all programs and systems implement the information security and privacy controls required by policy
8.2 Deputy CIO	The Deputy CIO participates in the Level III policy review process , as described in Appendix A.
8.3 Chief Technology Officer (CTO)	<p>The CTO is responsible for the following activities:</p> <ul style="list-style-type: none"> • Develop the TRA with the support of all components of the Office of Technology Solutions (OTS) and input from the CMS Emerging Edge Forum (CEEF) and CMS’s IT contractors • Approve all changes to the TRA
8.4 Management Officials	<p>Management officials, in their supervisory role, are responsible for the following activities</p> <ul style="list-style-type: none"> • Ensuring that employees, contractors, interns, etc. participate in the development and the review of CMS CIO policy in a timely manner, as appropriate • Informing users (employees, contractors, interns, etc.) of their rights and responsibilities, including the dissemination of the information in policy
8.5 Division of Policy, Program Integration, & Governance, Division Director	<p>The DPPIG division director is responsible for the following activities:</p> <ul style="list-style-type: none"> • Provides ongoing oversight and direction for the CIO policy program • Provides overall direction for the CIO policy function, including responsibilities for identifying and prioritizing policy needs • Resolves disputes. If conflicting comments are received and cannot be reconciled by the Policy Owner/SME, the conflicts must be escalated to the DPPIG division director for resolution
8.6 CMS CIO Policy	The CMS CIO Policy Officer is responsible for the following activities:

Role	Responsibility and Authority
Officer	<ul style="list-style-type: none"> • Facilitates and coordinates all CIO Policies developed by CMS or on behalf of CMS • Provides day-to-day support for the policy development function • Serves ex officio on policy development working groups • Determines the potential impact of policies, directives, guidance, best practices, etc. if made publicly available • Plans and executes policy education and awareness efforts • Manages an annual review and analysis of existing policies, standards, and guidelines for continued applicability and effectiveness • Provides interpretation of current policies in response to inquiries or specific incidents • Creates and distributes the CMS CIO Policy Comments Matrix
8.7 Policy Staff	<p>Policy staff are responsible for the following activities:</p> <ul style="list-style-type: none"> • Ensures appropriate stakeholder involvement in policy development • Conducts research and benchmarking for emerging policy development • Participates in policy development, vetting, and clearance, as requested
8.8 Policy Owner	<p>The Policy Owner is responsible for the following activities:</p> <ul style="list-style-type: none"> • Development and vetting of policies as described in <i>Appendix 1: CIO Policy Life Cycle</i>: • Monitoring compliance/metrics • Reviewing policies at least annually or more frequently as significant changes are identified that impact the policy. The term “significant change” refers to a change in federal legislation, mandates, directives, executive orders, and/or HHS policy that requires corresponding changes to be made to existing CMS policies. • Communication of updates to all stakeholders
8.9 Critical Partners	<p>Critical Partners are responsible for the following activities:</p> <ul style="list-style-type: none"> • Reviewing and approving new or revised policies as the second level of governance approval. For a list of Critical Partners, see Appendix 1: CIO Policy Life Cycle.

Role	Responsibility and Authority
	<ul style="list-style-type: none"> • Conducts research and benchmarking for emerging policy development • Composes the subject matter content of CIO policy and works with the CMS CIO Policy Officer to prepare the DRAFT CIO Policy and its review schedule. • Participates in policy development, vetting, and clearance, as requested
8.10 Office of Technology Solutions and Office of Enterprise Information	<ul style="list-style-type: none"> • Reviewing and approving new or revised policies as the first level of governance approval.
8.11 CMS Employees and Users of CMS IT Resources	<p>Users, including employees, contractors, interns, researchers, etc., are responsible for the following activities:</p> <ul style="list-style-type: none"> • Participating in the development of CIO policy or initiating CIO policy as the subject matter expert (SME), as needed • Responding timely to comments made regarding CIO policy during the CIO Policy Review Process where they are the SME • Adhering to the CMS CIO Policy Review Process schedule or timely requesting extensions of time to review • Providing timely comments during the CIO Policy Review Process and working collaboratively to address issues with the appropriate SME and the CMS CIO Policy Officer • Seeking guidance from their supervisors when in doubt about the implementation of a specific policy • Following Rules of Behavior in their use of IT resources (for example: Internet and email) and refraining from any practices which might jeopardize CMS computer systems and data files, including but not limited to resisting phishing attacks and encrypting / protecting sensitive data appropriately when transmitting, storing, or processing? • Familiarizing themselves with any special requirements for accessing, protecting and utilizing data, including but not limited to Privacy Act and Section 508 requirements, copyright requirements, and procurement-sensitive data • Adhering to all conditions set forth in Section 5, Policy

9 Metrics

Any metrics associated with this policy are established and tracked within the Division of Policy, Program Integration, & Governance (DPPIG).

10 Information and Assistance

Direct all questions, comments, suggestions or requests for further information to the CMS CIO Policy Officer at CIOPolicyFramework@cms.hhs.gov.

11 Applicable Laws/Guidance

[HHS OCIO Policy for Information Technology \(CIO\) Policy Development \(HHS-OCIO-2006-0004\)](#)

[Plain Language Act of 2010](#)

12 Reference Documents

Document #	Document Title
N/A	Comments Matrix
N/A	CIO Policy Template and Guide
N/A	Master List
N/A	Annual Review Schedule
N/A	Section 508 Policy
N/A	Architecture Change Request

13 Glossary

Term	Definition (or literal translation of acronym)
CIO Policy Document	CIO policy documents include policies, technical standards, directives, guidelines, and procedures that encompass topics related to information technology (IT) as well as information security and privacy.
Clearance	<p>The process of obtaining approvals by the appropriate CMS staff members before a CIO policy, standard, or directive is approved for dissemination.</p> <p>Clearance must be appropriate for the type of document under review and should balance the concerns of quality and timeliness. This guidance has been developed to promote consistent clearance procedures throughout CMS that ensure that the highest quality reviews are performed in a reasonable amount of time.</p> <p>Clearance is not a forum for extensive peer review or for policy debate. Such discussions belong in the pre-clearance phase. It is <u>not</u> the responsibility of the clearance official reviewing the information product to provide editing comments (e.g., comments on grammar and sentence structure). Review by a writer/editor may occur during the pre-clearance preparation and review phase, or during or after the clearance phase at the discretion of the center.</p> <ul style="list-style-type: none"> • Ensure high quality and appropriateness of written and visual communication • Engage the expertise of other units within the originating center, other centers, or CMS staff offices (e.g., Office of the General Counsel), as appropriate, for work that overlaps areas of responsibility • Obtain additional subject matter review when appropriate
CMS Information Technology (IT) Resources	Includes but is not limited to: staff, facilities, data, documents, laptops/personal computers and related peripheral equipment, software, network and web servers, telephones, facsimile machines, photocopiers, Internet connectivity and access to Internet services, email, and contractor-owned equipment accessing CMS IT resources.

Term	Definition (or literal translation of acronym)
CMS Emerging Edge Forum (CEEF)	The CEEF provides a forum for senior technical personnel across the Agency to share information and gain awareness regarding technology directives and strategy, industry trends and best practices.
Comments Matrix	A comprehensive matrix that accounts for all comments made by the reviewers regarding their review of a CMS CIO policy, standard, guideline, or procedure. The Comments Matrix is maintained for historical purposes.
Guidelines	<p>CIO Guidelines provide guidance and best practices relative to a particular topic. They may accompany, interpret, or provide guidance for implementing CIO policies, or may provide guidance to various CMS IT Life Cycle activities.</p> <p>Guidelines are recommended best practices but are not required to be in compliance with policy. A guideline aims to streamline particular processes according to a set routine or sound practice. By definition, following a guideline is never mandatory. Guidelines are not binding and are not enforced. Some CMS IT guidelines are referred to as “Practices Guides”.</p>
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data.
Policy	<p>A document predicated on oversight (Congressional mandates; legislation; Office of Management & Budget (OMB); Government Accountability Office (GAO); General Services Administration (GSA); National Archives Records Administration (NARA); etc.-this is not an all-inclusive list) requirements or Department/Agency authority that describes the “what” and the “when” certain actions must be taken in order to move an organization into compliance.</p> <p>Policy requires a certain level of measurement to determine where the organization is and how far from the end-state goal/requirement one is starting. Policy describes the specific tasks that need to be accomplished, much like a work breakdown structure (WBS), without stating “how” those tasks are accomplished.</p>

Term	Definition (or literal translation of acronym)
Procedures	A document that explains “how” policy must be achieved by describing the specifics of the tasks, the steps needed to be taken to achieve the goal, to satisfy the end state requirement.
Subject Matter Expert (SME)	A person or persons in a functional area who presents content material regarding the policy subject area.
Work Breakdown Structure (WBS)	A decomposition of the planned work effort into specific phases, tasks, activities, milestones, and deliverables necessary to accomplish project objectives. A WBS is a task-oriented or deliverable-oriented grouping of identified elements or components of a project, which organizes and defines the total scope of the project.

Appendix 1: CIO Policy Life Cycle

CIO Policy Governance identifies the different levels of governance review and vetting of draft or substantially revised policies, directives, guidelines, procedures, and technical standards.

The CIO policy life cycle process applies to all agency-level CIO guidance including policies, technical standards, directives, guidelines, and procedures. Directives, guidelines, and procedures may require fewer approvals than formal policies and standards.



CIO policy is developed by Subject Matter Experts (SMEs) who are responsible for composing the subject matter content of the CIO policy and working with the CMS CIO Policy Officer to prepare the DRAFT CIO Policy and its review schedule. It is recommended that all CIO policy development, when practicable, be a collaborative effort with all stakeholders and CMS critical partners in order to leverage the knowledge that an Integrated Project Team (IPT) can lend.

Stakeholders/critical partners who have first-hand knowledge or expertise of the subject matter, if not part of the IPT, must be conferred with and given the opportunity for first review of the document before it begins the formal CIO policy review process. All CIO policies written by or on behalf of CMS must comply with the formal CIO Policy Vetting and Clearance Process (described on page 16).

Please note: The Initiation, Planning, and Development activities described in the following sections do not apply to the TRA; instead, the TRA must follow the established process for document development specified in the [TRA Architecture Change Request Process Supplement](#).

Initiation and Planning Phase Activities

- Identify Need: Identify compelling need for new or updated policy/guidance. Drivers may include new regulatory requirements, technology developments, operational needs, and identification of current issues or gaps. The request may come from any CMS employee or contractor but must have the approval of CMS senior leadership prior to moving forward with developing/updating CIO policy.
- Determine whether the need should be satisfied by a policy, guideline, directive, standard, or procedure
- Start Change Management process
- Identify policy owner/sponsorship, stakeholders, SMEs, and other workgroup members and their relevant roles
- Prioritize and schedule policy work

Development Phase Activities

- Create draft policy (or guidelines, standards, procedures, directives); alternatively, make revisions to existing policy
- Distribute to workgroup members for initial review and input
- Incorporate initial input
- CIO Policy Officer reviews the DRAFT for content, format and consistency with other existing CIO policies

CIO Policy Vetting and Clearance Process

The purpose of the CIO Policy Vetting and Clearance Process is to ensure that all CIO policies, standards, and directives authored by CMS (or on behalf of CMS) and approved by the CIO are:

- (1) Of the highest quality
- (2) Technically accurate
- (3) Useful to the intended audience

Vetting and clearance should be appropriate for the type of document under review and should balance the concerns of quality and timeliness. This process promotes consistent clearance procedures throughout CMS that ensure that the highest quality reviews are performed in a reasonable amount of time.

The CIO Policy Officer initiates and oversees the formal CIO Clearance Process summarized below. Minimally, all new or substantially revised CIO policies, standards, and directives must have four levels of review:

- **Level I Review: OEI and OTS Group Directors**
 - CIO Policy Officer initiates the Level I Review by distributing Draft policy and blank Comments Matrix to reviewers.
 - OEI and OTS Group Directors have ten business days to review and comment on policy
 - All comments received by the CIO Policy Officer are forwarded to the Policy Owner/SME for review and assessment. If conflicting comments are received and cannot be reconciled by the Policy Owner/SME, the conflicts must be escalated to the DPPIG Division Director for resolution.
 - Policy Owner/SME incorporates feedback, where appropriate, and updates Comments Matrix. The SME provides comment disposition to each responder in the form of:
 - Accepted as presented
 - Accepted but modified, or

- Not accepted (and why)
- After changes or updates are complete, the CIO Policy Officer initiates the Level II review
- **Level II Review: Critical Partners.** Critical Partners include (but are not limited to): Enterprise Architecture (EA), Information Security, Privacy, Acquisition, Section 508, CPIC, Performance, Records Management, OOM/Labor Relations, Office of General Council (OGC), Technical Review Board (TRB), Internal CMS Emerging Edge Forum (CEEF) Members
 - CIO Policy Officer initiates the Level II Review by distributing updated Draft policy and blank Comments Matrix to reviewers.
 - Critical Partners have ten business days to review and comment on policy
 - All comments received by the CIO Policy Officer are forwarded to the Policy Owner/SME for review and assessment. If conflicting comments are received and cannot be reconciled by the Policy Owner/SME, the conflicts must be escalated to the DPPIG Division Director for resolution
 - Policy Owner/SME incorporates feedback, where appropriate, and updates Comments Matrix. The SME provides comment disposition to each responder in the form of:
 - Accepted as presented
 - Accepted but modified, or
 - Not accepted (and why)
 - After changes or updates are complete, the CIO Policy Officer initiates the Level III review

Note: Levels I and II reviews may be combined for expediency. Review times may be expanded beyond the recommended ten days (for complex material such as technical standards) or compressed (for time-sensitive material such as urgent directives).

- **Level III Review: CMS CIO Review and Approval**
 - The CMS CIO Policy Officer prepares the CIO policy approval package, which includes the completed Comments Matrix and the updated CIO Policy. (Note: The Comments Matrix serves as background material for the CIO to review.)
 - The CMS CIO Policy Officer forwards the CIO policy approval package to the co-signatories and the Deputy CIO for review and approval. Once approved by the co-signatories and the Deputy CIO, the approval package is forwarded to the CIO for final approval. Co-signatories may include the OTS Director/Deputy CIO, CISO, CTO, Senior Official for Privacy, and/or other members of CMS senior leadership, as appropriate.
 - The CIO approves and signs (or rejects with comments) ALL policies, technical standards, and directives.
 - After receiving CIO approval, the CIO Policy Officer initiates the Level IV review.

- **Level IV Review:** Strategic Work Information Folder Transfer System (SWIFT) Review. Includes senior leadership in all CMS Offices and Centers.
 - CIO Policy Officer initiates Level IV Review by forwarding the approved policy to OEI Business Operations Staff (BOS) for final vetting using SWIFT.
 - SWIFT reviewers have five business days to review and comment on policy
 - All comments received by the CIO Policy Officer are forwarded to the Policy Owner/SME for review and assessment. If conflicting comments are received and cannot be reconciled by the Policy Owner/SME, the conflicts must be escalated to the DPPIG Division Director for resolution.
 - Policy Owner/SME incorporates feedback, where appropriate, and updates Comments Matrix. The SME provides comment disposition to each responder in the form of:
 - Accepted as presented
 - Accepted but modified, or
 - Not accepted (and why)

Once the DRAFT CIO policy has effectively cleared CMS via review levels I through IV of the CIO Policy Vetting and Clearance Process, all appropriate updates are made, and the SME has addressed all the comments received, the CIO Policy Officer places the document under version control and performs rollout activities.

Minor revisions that do not change the substance of a policy (e.g., correcting grammatical or spelling errors, changing links, changing references to other policies or documents, changing position titles, etc.) can be addressed between the Policy Owner and the CIO Policy Officer without completing the formal vetting and clearance process.

Requests for Extensions of Time

- Requests for extensions of time to review are made to the CMS CIO Policy Officer via email prior to the review due date and are reviewed and approved/disapproved by the CMS CIO Policy Officer. It is the responsibility of the CMS CIO Policy Officer to ensure that the extensions of time for review are managed timely and that comments received are forwarded to the SME for disposition

Rollout Activities

- The CIO Policy Officer has 30 calendar days from the date the policy is signed by the CIO to:
 - Post the policy on the CMS website
 - Execute policy awareness and communications plan
 - Conduct educational activities, when appropriate
 - Initiate Maintenance activities

Maintenance Activities

- The Policy Owner/SME performs the following ongoing maintenance activities:
 - Monitors, measures, and evaluates compliance and effectiveness of implemented guidance
 - Reviews and updates according to posted review schedule
 - Revokes policy, when appropriate (see Section 5.4.1 Policy Revocation)

Appendix 2: CIO Policy Framework Structure

Document Type	Purpose	Applicability	Approval Authority	Review Cycle	Other Characteristics
CMS CIO Policies	<ul style="list-style-type: none"> • Have broad application throughout CMS • Articulates CMS’ vision, strategy, and core values as they relate to the management and use of information and CIO resources • Guides CMS’s decisions and directs individual behavior • Supports and enhances CMS’ mission • Clarifies requirements and exceptions • Ensures compliance with applicable laws and regulations • Helps manage risk to the Agency • Helps promote operational efficiency and consistency 	<ul style="list-style-type: none"> • CMS-wide, all Offices and Centers • All CMS employees, researchers, and organizations conducting business for and on behalf of CMS through contractual relationships 	CIO	Reviewed and updated per published review schedule or more frequently as significant changes are identified.	<ul style="list-style-type: none"> • Mandatory • Independent of specific technologies • Short, concise, clear • Must be implementable and enforceable • Accountability for implementation must be specified • Includes definition of terms (that are consistent across policies) • Links to templates and other related guidance.
CMS Technical Standards (Technical Reference Architecture - TRA)	<ul style="list-style-type: none"> • Articulates the technical architecture of the CMS Processing Environments • Assists all agency business partners in developing to, transitioning to, and maintaining the CMS Processing Environments in accordance with CMS’s enterprise technical architecture • May accompany, interpret, or specify requirements for implementing CIO policies, policy aspects, and the CMS Acceptable Risk Safeguards • Serves to accomplish compliance or risk mitigation • May specify rules for using a specific IT Service • Provides guidance to all CMS Expedited Life Cycle (XLC) activities 	<ul style="list-style-type: none"> • CMS-wide, all Offices and Centers • All CMS employees, researchers, and organizations conducting business for and on behalf of CMS through contractual relationships when using CMS IT resources. 	• CTO and CIO	Reviewed and updated per published review schedule or more frequently as significant changes are identified.	<ul style="list-style-type: none"> • Mandatory • The TRA foundation document focuses on technical architecture definition and alignment with Federal Enterprise Architecture (FEA) models. • The CMS TRA supplements focus on engineering detail to aid in consistent development and implementation within CMS environments. • May address specific technologies • Links to templates and other related guidance.

CMS CIO Policy Framework

Document Type	Purpose	Applicability	Approval Authority	Review Cycle	Other Characteristics
CIO Directives	<ul style="list-style-type: none"> Allows the CIO to respond to identified gaps in CMS policy and instruction. CIO Directives may require action or may be for informational purposes to help clarify existing policy. 	<ul style="list-style-type: none"> CMS-wide, all Offices and Centers All CMS employees and organizations conducting business for and on behalf of CMS through contractual relationships when using CMS CIO resources. 	CIO	Reviewed and updated per published review schedule or more frequently as significant changes are identified.	CIO Directives may also serve as a stop-gap to provide immediate guidance while a policy is being developed/updated, vetted, and approved.
CIO Guidelines	<ul style="list-style-type: none"> Provides guidance and best practices relative to a particular CIO topic May accompany, interpret, or provide guidance for implementing CIO policies or policy aspects 	<ul style="list-style-type: none"> CMS-wide, all Offices and Centers All CMS employees and organizations conducting business for and on behalf of CMS through contractual relationships when using CMS CIO resources. 	Applicable authority	Reviewed and updated per published review schedule or more frequently as significant changes are identified.	<ul style="list-style-type: none"> Not mandatory, may provide alternative approaches May depend on specific technologies Generally high-level – do not include step-by-step process Typically reference a parent policy Template (link tbd)
Procedures	<ul style="list-style-type: none"> Detailed step-by-step instructions Also referred to as Standard Operating Procedures (SOPs) 	As stated	Applicable authority	Review annually	Must align to and be consistent with CIO policies and applicable standards
Lower-level policies, guidelines, standards, or processes	<ul style="list-style-type: none"> As defined above when unique Office/ Center/ Group/Division-level requirements exist. 	Limited applicability	Applicable authority	Review as appropriate	<ul style="list-style-type: none"> Out of scope for CMS CIO Policy Framework Needed only when lower-level unique situations need special handling Consistent with CMS CIO policies but may be more restrictive