



UNITED STATES DEPARTMENT OF COMMERCE

Information Technology (IT) Policy Development

Table of Contents

1.0 Purpose.....	1
2.0 Scope.....	1
3.0 Background	1
4.0 Applicable Authorities	1
5.0 Cancellation/Augmentation of Existing Policy	2
6.0 Policy Statement(s)	2
7.0 Overview: IT Policy Life Cycle Process	2
7.1 Identification, Planning, and Initiation	2
7.2 Development, Review, and Approval	3
7.3 Promulgate/Rollout	4
7.4 Compliance, Review and Maintenance.....	4
7.5 Policy Retirement.....	4
8.0 Roles and Responsibilities	4
8.1 Role of the DOC Chief Information Officer	4
8.2 Role of the Office of Policy and Governance	5
8.3 Role of Responsible Office Director.....	5
8.4 Role of Department Bureaus.....	6
9.0 Internal Office Relationship.....	6
10.0 Effective Date.....	6
11.0 Review Cycle.....	6
12.0 Point of Contact.....	6
Appendix A- Policy Format Requirements	8
Appendix B- Policy Style Requirements	10

-----**This page intentionally left blank**-----

1.0 Purpose

The purpose of this policy is to formalize the process by which Department of Commerce (DOC) Office of the Chief Information Officer (OCIO) develops and authorizes departmental IT policy. This policy captures the process of IT policy development, establishes a minimum standard for language, content, and format, and highlights key roles and responsibilities for those involved in departmental IT policy making.

2.0 Scope

This policy applies to each office within DOC OCIO and extends to all federal and contractor employees engaged in the development of departmental IT policy. This policy is not intended to alter, change, or otherwise negatively affect Bureau-specific policy development processes and/or practices.

3.0 Background

- 3.1** Per DOC OCIO Internal Memorandum, *Department Information Technology Policy Development*, June 24, 2021, the Director of the OCIO/Office of Policy and Governance (OPG) shall manage the Department's IT policy development process.
- 3.2** DOC OCIO office directors are to provide appropriate subject matter expertise and/or policy leads to develop, update, and maintain departmental IT policies.
- 3.3** This collaborative relationship is to ensure newly developed (or substantially revised) departmental IT policy is consistent, anticipated, and maintains appropriate levels of feedback and vetting throughout the life cycle of each policy.
- 3.4** Departmental IT policies have Department-wide application and carry departmental force and effect.

4.0 Applicable Authorities

- 4.1** The Privacy Act of 1974, P.L. 93-579.
- 4.2** The Freedom of Information Act, 5 USC Sec. 552.
- 4.3** Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources."
- 4.4** Federal Information Security Modernization Act of 2014 (FISMA).
- 4.5** Section 508 of the Rehabilitation Act of 1973, as amended in 1998 (29 U.S.C. 794d).
- 4.6** Department Organization Order (DOO) 15-23, *Chief Information Officer*, July 2017.
- 4.7** OCIO Information Technology Policy Development Memorandum (Internal), June 2021.

5.0 Cancellation/Augmentation of Existing Policy None.

6.0 Policy Statement(s)

- 6.1 As specified in Section 7.2 below, each OCIO office shall collaborate with OPG throughout the lifecycle of all DOC-wide IT policies.
- 6.2 All departmental IT policies must meet the minimum standards for content, language, format, and style as found at Appendices A and B: [Policy Format Requirements](#) and [Policy Style Requirements](#); respectively.
- 6.3 All departmental IT policies must be shared with the CIO Council for information and review, be properly vetted with the Bureaus, and receive Office of Human Resources Management (OHRM) and Office of General Counsel (OGC) evaluation before submission to the DOC CIO for approval.
- 6.4 Each OCIO office shall adhere to the requirements of this policy.

7.0 Overview: IT Policy Life Cycle Process

7.1 Identification, Planning, and Initiation

- 7.1.1 This policy development schema starts with a recommendation of a valid need for new (or substantially revised) departmental IT policy to the CIO/DCIO.
- 7.1.2 Anyone may identify the compelling need and recommendation for a new or updated policy. Drivers may include new regulatory requirements, technology developments, operational needs, and identification of current issues or gaps. Requests may come from any employee, Bureau, council, or functional area (e.g., Information Security) that determines a need.
- 7.1.3 Because of the variety of drivers and the differing supervisory structures and internal operating procedures that may exist within organizations, recommendations for new policies should be discussed with OPG and evaluated against other requirements, priorities, and existing policies to ensure a valid need exists and the proposed policy does not contradict or overlap existing policy instruments
- 7.1.4 With a valid need determined, the DOC CIO/ Deputy Chief Information Officer (DCIO) appoints an appropriate Responsible Office Director (ROD) within the DOC OCIO for policy analysis and development. At this point, the ROD is charged with sponsoring the policy throughout its lifecycle.
 - 7.1.4.1 The ROD may identify a Subject Matter Expert (SME) or Manager to help with policy development.
- 7.1.5 The ROD captures the desired behaviors and outcomes of the policy, identifies stakeholders and potential working group

members, examines the high-level impacts of the proposed policy, and establishes timelines and key milestones.

7.2 Development, Review, and Approval

- 7.2.1 The ROD team drafts an initial policy that considers items presented above (*estimated time frame 3 weeks*).
- 7.2.2 With the initial draft developed, OPG is consulted to provide relevant departmental policy and pertinent federal guidelines on Records Management (RM), Paperwork Reduction Act (PRA), Section 508 compliance, eGovernance, etc.
- 7.2.3 The ROD can decide to distribute the initial draft policy to a small group of stakeholders (i.e., fellow OCIO Directors, technical SMEs, etc.) for initial review and input. prior to the formal vetting process,
- 7.2.4 The ROD adjudicates and incorporates this feedback into the initial draft as appropriate. At this point the document becomes known as the Full Policy Draft (FPD) (*estimated time frame 3 weeks*).
- 7.2.5 The ROD shall share the FPD with the CIO Council membership for information and review.
- 7.2.6 The ROD also distributes the FPD via the DOC Data Call Management System (DCMS) to a larger group of stakeholders that include Bureaus, and other OS program offices for review and input (*estimated time frame: 2- weeks*).
- 7.2.7 The ROD then adjudicates and incorporates this feedback into the FPD as appropriate.
- 7.2.8 The ROD then routes the FPD to Office of Human Resources Management (OHRM) for the union consultation process. If OHRM determines union consultation is required, OHRM facilitates union consultation and the ROD reviews and adjudicates any comments received from the union(s).
- 7.2.9 The ROD then routes to OGC for legal review.
- 7.2.10 As applicable, feedback is adjudicated and incorporated (*estimated time frame: 2-4 weeks*).
- 7.2.11 The ROD routes the Final Draft (including attachments and any required high-level education and outreach plans) to OPG for a final procedural and format review, as well as assignment of an office tracking number.
- 7.2.12 OPG then forwards this completed package to OCIO Internal Controls for DOC CIO approval and signature.
- 7.2.13 The DOC CIO approves new departmental IT policy by electronic signature (*estimated time frame 1-2 weeks*).

7.3 Promulgate/Rollout

- 7.3.1 OPG then publishes the new IT policy on the OCIO departmental IT policy library at: <https://community.max.gov/x/xos7Sg>; and announces policy approval and upcoming training requirements and dates via the DCMS, the CIO Council, and DOC Broadcast message (*estimated time frame: within 1 week of CIO signature*).
- 7.3.2 The ROD conducts education and training activities in accordance with published milestones.
- 7.3.3 The ROD initiates implementation in accordance with published timelines.

7.4 Review and Maintenance

- 7.4.1 While OPG tracks the effective dates of all OCIO IT policies to determine those in need of review, the ROD is responsible for conducting the review of all assigned policies.
 - 7.4.1.1 The default review cycle is once every three years.
 - 7.4.1.2 Based on operational need, the ROD may adjust the review cycle. In such case, annotation will be made as outlined at Appendix A.
 - 7.4.1.3 The ROD reviews and implements modifications per specified policy review cycle.
 - 7.4.1.4 The ROD responds to questions and compliance related queries.

7.5 Policy Retirement

- 7.5.1 As part of the maintenance and review process policies may be identified as out-of-date and/or no longer required. The ROD will lead the retirement process, coordinating all retirement procedures closely with OPG. Policies identified for retirement will be retired via the same process by which they were approved.

8.0 Roles and Responsibilities

8.1 Role of the DOC Chief Information Officer or designee.

- 8.1.1 Maintains overall responsibility for departmental IT policy and IT policy development.
- 8.1.2 Makes final decisions on approval, amendment, or rejection of proposed departmental IT policy.
- 8.1.3 Designates appropriate OCIO ROD sponsor for proposed departmental IT policy.
- 8.1.4 Ensures regular collaboration between OPG and other OCIO offices throughout the IT policy development lifecycle process.

- 8.1.5 Ensures compliance and conformance with public laws, regulations, OMB, and Government Accountability Office (GAO) regulations, policies, standards, procedures, and instructions concerning departmental IT development.

8.2 Role of the Office of Policy and Governance

- 8.2.1 Provides overall direction for the IT policy function to include the policy development process, maintenance, and review.
- 8.2.2 Ensures adherence to CIO approved IT policy development schema.
- 8.2.3 Plans and executes IT policy education and awareness efforts.
- 8.2.4 Working with RODs, manages review and analysis of all existing departmental IT policies for continued applicability and relevance.
- 8.2.5 Guides ROD through IT policy development process by ensuring knowledge of and compliance with federal and departmental policies.
- 8.2.6 Provides IT policy format and style requirements as well as IT policy development best practices as required.
- 8.2.7 Promulgates (or rescinds) Enterprise IT policies as required.
- 8.2.8 Maintains management and departmental access to all departmental IT policies via OCIO Policy Library located at: <https://community.max.gov/x/xos7Sg>.

8.3 Role of Responsible Office Director

- 8.3.1 Collaborates directly with OPG in the development of departmental IT policy.
- 8.3.2 Creates, implements, and gains compliance for proposed departmental policy.
- 8.3.3 Examines the high-level impacts of the proposed policies.
- 8.3.4 Maintains a list of potential stakeholders to be involved at various stages in the IT policy life cycle process.
- 8.3.5 Ensures stakeholders are engaged throughout IT policy development to ensure appropriate perspectives are accounted for and incorporated into final versions of proposed policies.
- 8.3.6 Provides FPD to the CIO Council for review/information.
- 8.3.7 Along with OPG, manages review and analysis of assigned policies for continued relevance.
- 8.3.8 Responsible for the development, implementation, and retirement of assigned departmental IT policies.
- 8.3.9 Identifies a Subject Matter Expert if required.
- 8.3.10 Provides background and justification for new or revised policy.
- 8.3.11 Drafts initial policy document, capturing projected timelines, anticipated training requirements, and other support systems and key milestone events needed to meet new policy requirements.

- 8.3.12 Complies with IT policy minimum standards for content, language, format, and style as found at Appendices A and B: [Policy Format Requirements](#) and [Policy Style Requirements](#); respectively.
- 8.3.13 Coordinates directly with OPG, other office, and departmental staffs as required to ensure compliance with existing legislative and departmental policies.
- 8.3.14 Distributes the FPD to broader group of stakeholders via DCMS for final comment and approval.
- 8.3.15 Routes the FPD to OHRM for union consultation.
- 8.3.16 Routes the FPD to OGC for legal review.
- 8.3.17 Provides Final Draft to OPG for procedural review, assignment of tracking numbers, and subsequent forwarding to the CIO for review and signature.

8.4 Role of Department Bureaus

- 8.4.1 Permit select employees to participate in policy development and review as outlined below:
 - 8.4.1.1 Technical SMEs will be called upon to work with the ROD/RM in support of development of the initial draft as well as the FPD.
 - 8.4.1.2 Other Bureau identified employees will be called upon individually or as members of a working group to assist with development and review of the FPD.
- 8.4.2 Disseminate and implement departmental IT policy once approved by DOC CIO.
- 8.4.3 Implement Bureau-specific enhancements as required.

9.0 Internal Office Relationship: In summary, the ROD owns the policy and controls its content, and the OPG facilitates the comprehensive development and review of departmental IT policy.

10.0 Effective Date: This policy is effective upon the date of signature.

11.0 Review Cycle: The review cycle for this policy is set at 3 years.

12.0 Point of Contact. Questions or concerns regarding this policy should be directed to the OPG at ocio_opg@doc.gov

Issued By:

André V. Mendes
Chief Information Officer

Appendix A: Policy Format Requirements

Departmental IT policies shall follow the format requirements described below:

Format:

- 1. Cover Page:** Optional
- 2. Table of Contents:** Optional, generally used when written policy exceeds 10 or more pages (excluding appendices and diagrams). When used, a “Table of Contents” (TOC) may be used for both new and revised policy. TOCs have the page number “i” when used. Each chapter listed in the TOC contains the start page number for that chapter.
- 3. Nature of Changes:** Required for revised policy only. A Nature of Changes describes, by chapter, the specific changes that a revised policy conveys. Revised policies contain this additional Nature of Changes page, numbered as “ii” following the TOC.
- 4. Purpose:** Describes the specific reason(s) that the IT policy is being written. That detail is whatever internal or external force(s) prompted the IT policy.
- 5. Scope:** There are two standard statements in the “Scope”. The first regards to whom this policy applies: “This policy applies to all Department Operating Units, including the Office of the Secretary, and organizations conducting business for and on behalf of the Department through contractual relationships when using DOC IT resources.” The second, speaks to the effects of the policy (e.g., USPTO is exempt from the requirements of this policy).
- 6. Background:** Provides the author and/or the Subject Matter Expert with the opportunity to further clarify the need for the policy that is not mandated or legislative, as contained in the “Purpose” chapter. Perhaps there is a story, or some historic reference, that adds or further explains why this policy is being written.
- 7. Applicable Authorities:** Where specific and applicable overarching references are listed. This list also serves to backup and confirm the “Scope” statement.
- 8. Cancellation/Augmentation of Existing Policy:** As applicable, this statement describes which policies may have been rescinded or in what ways existing policies may have been strengthened or updated as a result of this policy.
- 9. Policy:** Where the specific subject tasks and requirements are delineated. The delta between the mandate’s end state and where DOC is addressed in specific terms, steps, and/or tasks that will achieve the desired goal/end state. This is the heart of the IT policy and it is where both the compliance and performance criteria are set.
- 10. Roles and Responsibilities:** Where each affected functional area and each level of management/executive involved in the process is described in relationship to this specific IT policy subject. This is where a functional area and/or the management/executive

develops, creates, manages, sponsors, approves, reviews, and performs a specific role in this subject IT policy process.

11. Summary Statement: Optional, used to succinctly summarize the main points of the policy.

12. Effective Date/Implementation: The effective date of most policies is the date the policy is approved by CIO signature. However, there may be separate and distinct dates of implementation based on published milestones and/or specific roles and responsibilities herein assigned.

13. Review Cycle: The default review cycle for most IT policies is set at 3 years. However, the RM may assess a different review cycle, annotating it here.

14. Information and Assistance: A brief statement describing where one can go to find help with this policy or to whom to direct questions and/or comments.

15. Glossary: Optional.

16. Appendices and/or Figures: Optional.

Appendix B: Policy Style Requirements

Departmental IT policies shall follow the style requirements described below:

- 1. Policy Type Style:** All policy text shall be in type style Times New Roman.
- 2. Policy Text Size** (excluding specific headers): All policy text size (excluding specific headers) shall use font size 12.
- 3. Header 1:** All “header 1” shall be bolded and in font size 14.
- 4. Header 2:** All “header 2” shall be bolded and in font size 12.
- 5. Chapter Sections:** All chapter sections shall be unbolded and in font size 12.
- 6. Subsections:** All subsections shall be unbolded, indented and in font size 12.
- 7. Pagination:** Page numbers are in the footer at the lower center of each page.
- 8. Footers:** Footers also contain the proper name of the policy, such as: OCIO Policy for XXXXXXXXXXXX in the lower right-hand corner of each page.