# CIOP CHAPTER 1351.40

# Common Operating Environment (COE) Services Management Policy

# TABLE OF CONTENTS

Section 40.1. Purpose ..... 1
Section 40.2. Background ..... 2
Section 40.3. Scope and Applicability ..... 3
Section 40.4. Policy ..... 4
Section 40.5. Roles and Responsibilities ..... 11
Section 40.6. Dates ..... 15
Section 40.7. Cancellations ..... 15
Section 40.8. Compliance ..... 15
Section 40.9. Waivers ..... 16
Section 40.10. Audit Procedures ..... 16
Section 40.11. Approval ..... 16
Appendix A – Definition of Terms ..... i
Appendix B – Legal Authorities and Guidance ..... ii

## Section 40.1. Purpose

The Department of Transportation (DOT) leverages Information Technology (IT) on a daily basis to achieve its mission of a safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life. However, traditional IT services can be duplicative across the Department, which wastes money and increases the time required to resolve service issues.

Sharing IT services allows the Department to rationalize IT investments, drive down costs and improve service. Departmental shared services are provided in a Common Operating Environment (COE) and managed by IT Shared Services (ITSS), a fee-for-service organization within the Office of the Secretary. COE customers are Departmental Operating Administrations and Secretarial Offices that pay according to Working Capital Fund (WCF)-established billing methodologies to leverage these services. ITSS is committed to supporting and working with participating customers to meet their business needs.

This document establishes the ITSS policy, roles, responsibilities and requirements outlined in Federal law and guidance, as well as Departmental plans including the 2014-2018 DOT Strategic Plan and the OCIO's Information Resource Strategic Plan.

(Table of Contents)

## Section 40.2. Background

ITSS is committed to providing business solutions through an IT infrastructure that allows customers to focus on managing their unique mission solutions and data.

Per OMB Memorandum M-11-29: Chief Information Officer Authorities, ITSS is the preferred provider of IT and infrastructure services for the Department. As the preferred provider, ITSS is committed to providing reusable and sharable services and products that obtain mission or support functionality at the best value to cost ratio whenever possible.

Through the Department's Administrative Working Capital Fund (WCF), ITSS provides IT shared services to COE customers. These services, critical to achieving the DOT's overall mission, include but are not limited to wide area network (WAN) services, email and messaging services, desktop computer management services, and service desk support.

As described in Office of Management and Budget Memorandum M-11-29, IT shared service opportunities include:

- IT infrastructure (e.g., data centers, networks, workstations, laptops, software applications, and mobile devices); and
- Enterprise IT services (e.g., e-Mail, web infrastructure, collaboration tools, security, identity and access management).

While the COE provides many critical services, it does not provide all the IT services that are required to support fulfillment of the customer missions; each customer must augment its COE-provided IT services to meet organization-specific needs. Enmeshing ITSS-provided services and customer-managed services can create challenges for both organizations, including:

- Ensuring that COE-provided IT services are of acceptable quality and performance standards while being cost effective in comparison to customer-provided services;
- Ensuring that customer mission-specific requirements drive the design and delivery of COE IT services via periodic reviews of the COE IT service catalog;
- Ensuring transparency of enterprise service delivery models and cost models; and
- Ensuring that services are designed to meet targeted objectives with tangible benefits (e.g., improved user experience, reduced costs, compliance with Federal standards, etc.).

ITSS recognizes that addressing these challenges requires attention to each stage of the service portfolio lifecycle as prescribed by the Information Technology Infrastructure

Library (ITIL)[1]. The five stages of service strategy, service design, service transition, service operation, and continual service improvement make up the full lifecycle of a service:

1) **Service Strategy:** Defines the IT strategy and policies, including why a customer should buy ITSS services; the pricing and chargeback models; allocation of resources and capabilities; and an assessment of strengths, weaknesses, priorities, and risks.
2) **Service Design:** Ensures that an agreed-upon level of service will be provided for IT services, and that future services are delivered at achievable levels.
3) **Service Transition:** Plans and coordinates resources to ensure the interwoven service strategy and service design are realized in service operations. This phase includes identifying, managing and controlling the risks of failure and disruption across transition activities.
4) **Service Operation:** Focuses on effective and efficient day-to-day operation of ITSS services including fulfilling user requests, resolving service failures, monitoring service center performance, and carrying out routine operational tasks.
5) **Continual Service Improvement:** Monitors service activities in an ongoing commitment to measure, report on, and improve operational activities.

(Table of Contents)

## Section 40.3. Scope and Applicability

This policy applies to ITSS employees and contractors and the services they provide, as well as DOT program offices, Federal employees, and contractors that currently participate in the COE. It also applies to non-customers who use this policy as a decision-making tool regarding becoming a COE customer. This policy refers to all DOT Operating Administrations and Secretarial Offices collectively as “DOT Components.”

All DOT Components are required to evaluate ITSS-offered services and eliminate them as a workable, cost-effective option before soliciting information on or implementing an alternative resource.

This policy applies only to the extent that such requirements and recommendations are consistent with the expressed language contained in the FAA authorization, FAA General Procurement Authority, and FAA Air Traffic Control Modernization Reviews.[2]

---

[1] The Information Technology Infrastructure Library (ITIL) is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. ITIL is published in a series of five core volumes, each of which covers an ITSM lifecycle stage. ITIL describes processes, procedures, tasks and checklists for delivering value. It allows the organization to establish a baseline from which it can plan, implement and measure to demonstrate compliance and to measure improvement.

[2] 49 U.S.C. §§ 106, 40110, 40121

The Office of Inspector General (OIG) is not a Component as defined in this policy, but will issue internal policies consistent with this policy and work with the DOT Chief Privacy Officer when consistent with OIG independence.

The DOT OCIO will develop and issue supplemental guidance as necessary to implement this policy in order to assist staff in conducting their responsibilities.

(Table of Contents)

## Section 40.4. Policy

### Service Strategy

The ITSS service portfolio management process governs COE investments across the enterprise and manages them for value.

The service portfolio is the complete set of services that are managed by ITSS. A COE service can be made up of IT systems within the overall DOT infrastructure including hardware, software, networks, environments, data, and applications.

The goals of the service portfolio management process are to communicate services, anticipate needs and changes, and maintain traceability to strategy and planning.

*Service Portfolio Management.*

Service Portfolio Management ensures the right mix of services to meet business needs.

40.4.1. ITSS shall produce and maintain an inventory of services available to COE customers. This inventory will consist of:

40.4.1.1. **Business services** define the customer view of COE services available and the business processes required for obtaining those services. This inventory shall be made readily available for customer review and comment.

40.4.1.2. **Technical services** define the details of COE services delivered to the customer and their relationships to supporting services. This inventory includes the details and current status of every service, regardless of operational status, including interfaces and dependencies. The technical services are not part of the customer view.

40.4.2. ITSS shall work with customers and the CIO Council to regularly review the business service catalog to maximize portfolio value, prioritize services and respond to customer comments on available services.

40.4.3. ITSS shall regularly review the technical service catalog to ensure it is accurate and reflects the current details, status, interfaces and dependencies of services that are being run, or being prepared to run, in the live environment.

40.4.4. ITSS shall provide COE services necessary to achieve the DOT mission and include them in the service portfolio.

40.4.5. ITSS shall communicate service changes and updates to the COE customers consistent with SLAs.

40.4.6. ITSS shall establish and implement a process for collecting and evaluating business users' awareness of services being provided.

40.4.7. ITSS shall make available Key Performance Indicators (KPIs) that reflect the status and progress of all service lifecycle activities.

40.4.8. ITSS shall retain all documentation in accordance with DOT Order 1351.28, Records Management Policy.

*Financial Management*

Financial Management coordinates budgeting, accounting and charging requirements for COE services. Financial management of the COE is conducted through the Working Capital Fund (WCF.) Any changes to billing rates or services that will effect resource utilization need to be approved by the WCF Steering Committee in addition to any oversight and governance bodies.

40.4.9. ITSS shall work with customers and the CIO Council to select technology solutions that meet COE needs and provide the best value to cost ratio.

40.4.10. ITSS shall take proactive measures to improve the level of service delivered wherever it is cost-justifiable to do so.

**Service Design**

ITSS service design ensures a consistent interface for COE customers. The service design includes DOT service targets and the management information to ensure those targets are met.

40.4.11. ITSS shall develop specific and measurable targets for COE services.

> 40.4.11.1. I TSS shall collaborate with customers and the CIO Council to determine service offerings, service agreements and costs that are mutually agreeable and communicate the agreed-upon COE service targets through Service Level Agreements (SLAs). These agreements will define, but are not limited to, service measurement standards, service goals, issue response and resolution standards, and issue prioritization criteria. SLAs shall also include service desk hours of operation, contact information, and alternate response options for critical issues outside of service desk hours.
>
> 40.4.11.2. ITSS shall monitor and measure service performance achievements of operational services against targets within SLAs.
>
> 40.4.11.3. ITSS shall review and revise SLAs as needed to ensure performance levels align with business requirements and agreed-upon targets.

40.4.12. ITSS shall document customer business needs, responsibilities and agreed-upon service levels in Service Level Requirements (SLR) that determine, negotiate and agree to requirements for new or changed services.

> 40.4.12.1. ITSS shall manage and review SLRs through the service lifecycle and incorporate SLR targets into SLAs for operational services.

40.4.13. ITSS shall identify stakeholder responsibilities prior to operational deployment of COE services.

40.4.14. ITSS shall make available and maintain up-to-date service level management document templates and standards.

*Customer Service*

Customer Service provides assistance and advice to customers who encounter issues with COE services.

40.4.15. ITSS shall establish a customer service model that addresses IT issue response and service requests based on severity and customer priority within agreed-upon time frames.

40.4.16. ITSS shall develop, maintain and operate a service desk and corresponding system for documenting, responding to and resolving service complaints.

40.4.17. ITSS shall conduct regular service reviews and initiate improvements through a service improvement plan when necessary and financially justified.

*Availability Management*

Availability Management defines, analyzes, plans, measures and improves the availability of COE services.

40.4.18. ITSS shall produce and maintain an appropriate and up-to-date availability plan that reflects the current and future needs of COE customers.

40.4.19. ITSS shall establish a notification process to provide sufficient notice to customers before any planned maintenance or service outages.

40.4.20. ITSS shall evaluate and resolve availability-related incidents and problems consistent with SLAs.

40.4.21. ITSS shall establish a response schedule for unplanned outages that includes notification to customers indicating expected time to resolution, and system and impacted customer identification.

40.4.22. ITSS shall define targets for availability, reliability and maintainability (ARM) for IT infrastructure components that underpin IT service and document the targets as a part of SLAs.

40.4.23. ITSS shall establish measures and reporting of ARM that reflect the business, user and organization needs.

40.4.24. ITSS shall regularly review IT service availability to identify and correct unacceptable levels.

> 40.4.24.1. In the case of unacceptable levels of availability, ITSS shall investigate the underlying reasons for unacceptable availability and work to correct them.

*Capacity Management*

Capacity Management aims to ensure that the capacity of COE services and the COE infrastructure is able to deliver the agreed service level targets consistent with SLAs.

40.4.25. ITSS shall produce and maintain an appropriate and up-to-date capacity plan that reflects the current and future needs of COE customers.

40.4.26. ITSS shall diagnose and resolve performance- and capacity-related incidents and problems.

40.4.27. ITSS shall assess and document the impact of changes to the capacity plan, and the performance and capacity of services and resources.

40.4.28. ITSS shall ensure that upgrades are budgeted, planned and implemented before SLAs and service targets are breached or performance issues occur.

*Continuity of Operations Planning (COOP) and Disaster Recovery*

Disaster Recovery and COOP allow the Department to address the steps to be taken in order to maintain operation of critical functions in the event of contingencies, losses, disruptions or disasters.

40.4.29. ITSS shall produce and maintain IT service continuity plans and IT recovery plans that support the overall business continuity plans of the organization.

40.4.30. ITSS shall ensure that continuity plans are maintained in line with changing business impacts and requirements.

40.4.31. ITSS shall establish a data backup process that ensures the recoverability of any data that may be lost or corrupted in the event of a disaster, equipment failure, and intentional or unintentional destruction of data.

40.4.32. ITSS shall ensure appropriate continuity and recovery mechanisms are put in place to meet or exceed continuity targets.

*Information Security Management*

Information Security Management ensures the confidentiality, integrity and availability of information, data and IT services within COE systems.

40.4.33. ITSS shall conduct regular risk analysis and management exercises, in conjunction with the security and risk management processes, to maintain COE services within an agreed level of risk.

40.4.34. ITSS shall ensure that COE services are secured in accordance with the Departmental Cybersecurity Policy.

40.4.35. ITSS shall ensure that information is complete, accurate and protected against unauthorized modification.

40.4.36. ITSS shall develop an incident monitoring and reporting process that includes actions taken to contain and eradicate issues, as well as any recovery, protection and post-incident activities.

40.4.37. ITSS shall ensure that information is available and usable when required and the systems that provide the information can appropriately resist attacks and recover from or prevent failures.

40.4.38. ITSS shall schedule and complete required security reviews, audits and penetration tests by or before the scheduled deadlines.

*Contract Management*

Contract Management ensures that all contracts support COE needs and that all suppliers meet their contractual commitments.

40.4.39. ITSS shall identify the need for any new contracts, including the method of procurement, evaluation criteria and alternatives.

40.4.40. ITSS shall manage and document contract performance to ensure agreed-upon targets are met or exceeded.

40.4.41. ITSS shall regularly review contract performance and determine if contracts need to be renegotiated, renewed, terminated or transferred.

**Service Transition**

Through service transition management, ITSS ensures that strategies and designs are executed in operations by identifying, managing and controlling the risks of failure and disruption across transition activities. Transition activities include initiating new services, changing existing services or terminating services. Transition management improves the COE's ability to handle high volumes of change and releases.

40.4.42. ITSS shall plan and coordinate resources to successfully complete a new, changed or terminated service activity within the predicted cost, quality and time estimates.

40.4.43. ITSS shall create and implement a clear and comprehensive service transition strategy that enables customers to change projects to align activities with service transition activities.

*Change Management*

Change management allows the COE to make beneficial changes to services and systems with minimum disruption to the customer.

40.4.44. ITSS shall establish and implement a system for prioritizing and responding to customer change proposals to meet business timescales and reduce the time to restore service.

40.4.45. ITSS shall create and implement a process for tracking and documenting changes throughout the service lifecycle.

*Asset and Configuration Management*

Asset and configuration management establishes and maintains consistency of COE service performance, functional and physical attributes when compared with original requirements, design and operational information.

40.4.46. ITSS shall ensure that services, systems and/or products, collectively referred to as COE assets, are identified, baselined and maintained, and that changes are controlled and documented.

40.4.47. ITSS shall create and maintain a complete inventory of COE assets and the parties responsible for their control.

40.4.48. ITSS shall support efficient and effective service management by maintaining configuration information on the historical, planned and current state of COE assets.

40.4.49. ITSS shall create and implement a process to minimize the number of quality and compliance issues caused by improper configuration of COE assets.

*Release and Deployment Management*

Release and deployment management activities include planning, scheduling and controlling releases to ensure that the COE environment is protected and correct components are released.

40.4.50. ITSS shall create, implement and communicate clear and comprehensive release and deployment plans that enable customers to align business activities.

40.4.50.1. ITSS shall include a release and deployment management phase where customer input is collected and incorporated into release and deployment activities.

40.4.51. ITSS shall establish a process to ensure release packages can be built, installed, tested and deployed efficiently to a deployment group or target environment successfully and on schedule.

40.4.52. ITSS shall ensure any new or changed service can deliver agreed-upon service requirements.

40.4.52.1. ITSS shall notify users in advance of any release or service change that may impact service.

40.4.52.1.1. ITSS shall take steps to ensure minimal downtime to users during a release or service change.

40.4.53. ITSS shall create and implement a service validation and testing process to be executed throughout the service lifecycle.

40.4.54. ITSS shall validate that a service meets specifications and conditions of use and will deliver required performance prior to releasing the service.

40.4.55. ITSS shall establish a process to evaluate and document the intended effects of a new service, service change or termination, and measure the evaluation results against intended outcomes.

*Knowledge Management*

Knowledge Management allows ITSS to gather, analyze, store, and share knowledge and information to improve efficiency.

40.4.56. ITSS shall create and implement a knowledge management strategy that ensures reliable and secure information and data is available throughout the service lifecycle.

40.4.57. ITSS shall develop and maintain a comprehensive knowledge management repository.

40.4.58. ITSS shall confirm that customer and stakeholder requirements for new or changed services are correctly defined.

40.4.59. ITSS shall develop standard operating procedures and policies memorializing best practices.

**Service Operation**

Service operation management ensures that COE services are delivered effectively and efficiently on a day-to-day basis and throughout the service lifecycle. This includes fulfilling user requests, resolving service failures, fixing problems, and carrying out routine operational tasks.

*Incident Management*

Incident management involves monitoring COE services and systems, evaluating any incidents that occur, and restoring normal COE service consistent with SLAs.

40.4.60. ITSS shall ensure services are constantly monitored, and will filter and categorize service issues or interruptions in order to decide on appropriate actions.

40.4.61. ITSS shall manage and document incidents in order to return the IT service to users as quickly as possible.

40.4.62. ITSS shall develop and implement a methodology to monitor trends to prevent incidents.

*Request Fulfillment*

Request fulfillment is a function of customer service wherein the help desk responds to service requests or requests for information.

40.4.63. ITSS shall establish and implement a process for fulfilling help desk service requests, including escalation tiers for critical issues and documentation of the request lifecycle.

*Access and Identity Management*

Access and identity management ensures authorized users have full access to COE services and systems needed to perform their jobs.

40.4.64. ITSS shall establish and implement an identity management process to grant authorized users the right to use a service while preventing access to non-authorized users.

40.4.65. ITSS shall determine the optimal baseline image and establish an image lifecycle management plan that dictates how and when images are replaced.

*COE Operations Management*

COE operations management addresses the physical location, safety and maintenance of COE infrastructure.

40.4.66. ITSS shall monitor and control COE services and their underlying infrastructure, including day-to-day routine tasks related to the operation of infrastructure components and applications.

40.4.67. ITSS shall comply with all environmental and physical access requirements at any location containing COE assets, including standards for power and cooling, building access management, and environmental monitoring.

40.4.68. ITSS shall provide technical expertise and support for the management of COE infrastructure.

**Continual Service Improvement**

ITSS uses continual service improvement management, including ongoing customer engagement, to learn from past successes and failures by updating the effectiveness and efficiency of IT processes and services while maintaining communication with customers.

40.4.69. ITSS shall review business services and infrastructure services on a regular basis to improve service quality where necessary and to identify more economical ways of providing a service where possible.

40.4.70. ITSS shall evaluate processes on a regular basis. This includes identifying areas where the targeted process metrics are not reached and holding regular audits, maturity assessments and reviews.

40.4.71. ITSS shall define specific initiatives aimed at improving services and processes, based on the results of service reviews and process evaluations.

40.4.72. ITSS shall verify whether improvement initiatives are proceeding according to plan and introduce corrective measures where necessary.

(Table of Contents)

## Section 40.5. Roles and Responsibilities

This section defines the roles key to implementing the Services Management Policy across the DOT and specific responsibilities associated with each role. Provided below is a summary listing of the roles and the levels in the organization where they reside.

**Department Level**

- Department Chief Information Officer
- Department Associate Chief Information Officer for IT Shared Services
- Department Chief Information Security Officer
- Office of General Counsel
- Senior Procurement Executive
- Working Capital Fund
- CIO Core Council
- Department of Transportation COE Steering Committee

**Component Level**

- Component Administrator
- Component Chief Information Officer

**DOT-Wide**

- DOT Employees and Contractors

**Department Level**

40.5.1. Accountability for directing DOT's IT functions resides with the DOT Chief Information Officer (CIO). In addition to responsibilities listed elsewhere in Departmental policy, the **DOT Chief Information Officer (CIO)** will:

40.5.1.1. Appoint a Department Associate Chief Information Officer for IT Shared Services to assist with implementation, evaluation and administration issues for COE service management.

40.5.1.2. Provide advice and other assistance to the head of the executive agency and other senior management to ensure that information technology is acquired and COE services are managed effectively and efficiently.

40.5.1.3. Provide for the selection of information technology investments, the management of such investments, and the evaluation of the results of such investments.

40.5.1.4. Maintain a central policy-making role in the organization's development and evaluation of legislative, regulatory and related policy proposals involving shared services.

40.5.1.5. Ensure that information and delivery of services meets Departmental accessibility requirements for COE business operations.

40.5.2. The Department Associate Chief Information Officer for IT Shared Services serves as the primary point of contact for this policy and is assigned responsibility for the operationalization of the IT Shared Services program, including operational responsibilities of the CIO. The **Department Associate Chief Information Officer for IT Shared Services (Associate CIO for ITSS)** will:

40.5.2.1. Serve as the operational lead for all COE programs, initiatives and services.

40.5.2.2. Provide the means for senior management to obtain information regarding the progress of an investment in the COE system.

40.5.2.3. Design and implement a process for maximizing the value and assessing and managing the risks of COE acquisitions.

40.5.2.4. Exercise a central role in overseeing, coordinating and facilitating the organization's COE activities. This role includes establishing and periodically reviewing/updating the organization's COE service management processes and procedures to ensure that they are comprehensive and current.

40.5.2.5. Engage in close collaboration with key organization officials, including the CIO, Chief Information Security Officer (CISO), business owners, privacy personnel and others, to discuss new initiatives and integration of COE service management throughout the System Development Life Cycle.

40.5.2.6. Provide for and oversee the development, implementation and maintenance of COE standards and processes, including but not limited to all COE service portfolios.

40.5.2.7. Focus on eliminating duplication and rationalizing Departmental IT investments, including IT infrastructure, enterprise IT systems, identity and access management, security, web infrastructure, and business systems.

40.5.3. The **Departmental Chief Information Security Officer (DOT CISO)** will:

40.5.3.1. Advise and support the Associate CIO for ITSS in all security-related aspects of COE service management.

40.5.3.2. Provide oversight and guidance with respect to FISMA implementation and related audits.

40.5.4. The **DOT Office of General Counsel (OGC)** will consult with the Associate CIO for ITSS to:

40.5.4.1. Identify the laws, regulations and internal policies that apply to COE service management and provide guidance on the impact or implementation requirements of the same.

40.5.4.2. Participate in the drafting process for COE service management notices, information collections and rulemakings.

40.5.5. The **Office of the Senior Procurement Executive (SPE)** will:

40.5.5.1. Partner with the Associate CIO for ITSS to develop and implement COE service management contract clauses for incorporation in all current and future contracts and covered grants.

40.5.5.2. Promote the appropriate use of the required clauses in all applicable contracts.

40.5.5.3. Ensure contracting officers (COs) enforce the requirements of COE service management clauses.

40.5.6. The **Working Capital Fund Steering Committee (WCF Steering Committee)** will work with the DOT OCIO, the Chief Information Officers Core Council (CIO Core) and the Associate CIO for ITSS to:

40.5.6.1. Establish a standard Working Capital Fund (WFC) billing methodology for services provided to customers within the COE.

40.5.6.2. Ensure IT portfolio analysis is an integral part of the yearly budget process for the department.

40.5.6.3. Ensure that no funds appropriated for shared services shall be transferred to the Working Capital Fund without majority approval of the WCF Steering Committee and approval of the Secretary.

40.5.7. The **Chief Information Officers Core Council (CIO Core)** membership consists of Chief Information Officers from across the department. The CIO Core shall:

40.5.7.1. Approve or disapprove COE Steering Committee recommendations.

40.5.8. The **Department of Transportation COE Steering Committee (COESC)**, chartered under delegated authority from the Secretary of the DOT and the DOT CIO leadership, serves as the DOT's inter-organizational body to conduct IT shared service strategic planning and to perform COE IT shared service program oversight. Consistent with its charter, the COESC will:

40.5.8.1. Provide recommendations to senior management on major DOT IT Shared Services Program initiatives and the management of DOT's IT Shared Services Program.

40.5.8.2. Provide recommendations on strategic IT decisions and resource allocations to the DOT CIO Core Council.

40.5.8.3. Annually review the DOT IT Shared Services Program and make change recommendations to the DOT CIO Core Council.

40.5.8.4. Make recommendations on prioritization of ongoing and new efforts and initiatives, as well as supporting the inclusion of necessary resources through the planning and budgeting process.

40.5.8.5. Monitor the effectiveness of COESC recommendations after implementation to continue to refine and improve the ITSS COE Service Management program.

40.5.8.6. Review any Departmental IT-related strategic plans and recommend updates as necessary.

40.5.8.7. Review the work products produced by the COESC working groups.

**Component Level**

40.5.9. Accountability for IT functions of the Component and its groups resides with the Component Chief Information Officer. In addition to responsibilities listed elsewhere in Departmental policy, the **Component Chief Information Officer (Component CIO)** will:

40.5.9.1. Evaluate and rule out ITSS-provided services before seeking alternative IT systems or solutions.

40.5.9.1.1. Evaluate any service that is not currently provided by ITSS but is within the scope of potential services to determine if ITSS could provide the service in accordance within the timeline of business needs.
40.5.9.1.2. Information the DOT OCIO of any current IT solutions being used

40.5.9.2. Ensure that investments align to enterprise objectives of minimizing duplicative services and maximizing the use of shared services.

40.5.9.3. Designate a Component representative responsible for coordination, escalation and testing of COE services.

**DOT-Wide**

40.5.10. All **DOT Employees, Contractors, Trainees and Interns** leveraging COE services shall:

40.5.10.1. Comply with all ITSS-established processes and procedures for the selection, use, maintenance and documentation of COE services.

(Table of Contents)

## Section 40.6. Dates

40.6.1. The effective date of this policy is the date the policy is approved and signed.

40.6.2. In accordance with the CIOP and the DOT Order Directive Process, this chapter shall be reviewed annually and validated by the Policy Owner. The directive content shall be annually reviewed to ensure it has clear intent, contains the right material and complies with the IT Directive Publication Process. Roles and responsibilities shall be reviewed and updated on a quarterly basis.

(Table of Contents)

## Section 40.7. Cancellations

40.7.1. There are no services management directives currently in place, although there have been a number of informational DOT communications regarding services management. This directive supersedes and cancels all earlier communications specific to this topic.

(Table of Contents)

## Section 40.8. Compliance

40.8.1. COE customers must comply with and support the implementation of the Services Management Policy, to include compliance with Federal requirements and programmatic policies, standards and procedures. This policy applies to all DOT Components (and organizations conducting business for and on behalf of the Department through contractual relationships when using DOT IT resources) leveraging COE services. This policy does not supersede any other applicable law, higher-level agency directive, or existing labor management agreement in place as of the effective date of this policy.

40.8.2. Departmental officials must apply this policy to employees, contractor personnel and interns and other non-government employees leveraging COE services. All DOT Components using or operating information systems on behalf of the COE are also subject to this Departmental Services Management Policy.

40.8.3. ITSS may revoke any user's access privileges at any time for policy or standards violations that may potentially disrupt the normal delivery of ITSS services.

40.8.4. Depending on the severity of non-compliance, and at the discretion of management, consequences for non-compliance will apply until satisfactory corrective actions have been taken. Consequences may include, but are not limited to, any, or a combination of the following:

40.8.4.1. Reprimand.

40.8.4.2. Suspension of ITSS-provided services.

40.8.4.3. Information system disconnection.

(Table of Contents)

## Section 40.9. Waivers

40.9.1. Compliance with this policy is mandatory for COE customers.

40.9.2. COE customers may request that the Associate CIO for ITSS grant a waiver of compliance based on a compelling business reason. In addition to an explanation of the waiver sought, the request must include: (1) justification, (2) measures taken to ensure implementation of IT management principles, (3) length of requested waiver period and (4) projected milestones to achieve compliance. The Associate CIO for ITSS will provide a written waiver or justification for denial.

(Table of Contents)

## Section 40.10. Audit Procedures

40.10.1. In order to ensure the Department provides appropriate accountability for services management, and that the Associate CIO for ITSS provides active support and oversight of monitoring and improvement of the Departmental Services Management Program, the Associate CIO for ITSS must:

40.10.1.1. Develop and implement an oversight and compliance function to provide the required guidance and reviews to meet department- and government-wide services management requirements;

40.10.1.2. Conduct annual compliance reviews of DOT Component Services Management Programs;

40.10.1.3. Develop and manage the Departmental Services Management Program, reporting progress to the DOT CIO and Secretary of Transportation;

40.10.1.4. Monitor COE customer efforts to identify and address weaknesses in their respective Services Management Programs; and

40.10.1.5. Ensure that corrective actions identified as part of the assessment process are tracked and monitored until findings are corrected.

40.10.2. DOT will conduct an audit of the DOT COE Services Management Policy program as required by DOT Order 1351.1, IT Directives Management.

(Table of Contents)

## Section 40.11. Approval

RICHARD MCKINNEY

Digitally signed by RICHARD MCKINNEY
DN: c=US, o=U.S. Government, ou=DOT Headquarters, ou=OSTHQ, cn=RICHARD MCKINNEY
Date: 2015.02.20 17:20:36 -05'00'

Richard McKinney
DOT Chief Information Officer

(Table of Contents)

# Appendix A – Definition of Terms

**Common Operating Environment:** An opt-in organization providing fee-for-service delivery of common IT services to DOT Components.

**Information System:** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: NIST SP 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems)

**Information Technology:** Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency; equipment used by the executive agency directly or by a contractor under a contract with the executive agency that requires the use – (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. (Source: Clinger Cohen Act of 1996)

**Service Level Agreement (SLA):** An agreement between ITSS and the customer that defines, but is not limited to, service measurement standards, service goals, issue response and resolution standards, and issue prioritization criteria.

**Service Portfolio:** The complete set of services that are managed by ITSS. A COE service can be made up of IT systems within the overall DOT infrastructure including hardware, software, networks, environments, data, and applications.

**System Owner:** The key POC for the system who is responsible for coordinating SDLC activities specific to the system. It is important that this person have expert knowledge of the system capabilities and functionality. (Source: NIST 800-18rev1)

**System Development Lifecycle (SDLC):** The method of protecting information and information systems by integrating security and privacy into every step of the system development process. The multistep process starts with initiation, analysis, design, and implementation, and continues through the maintenance and disposal of a system.

# Appendix B – Legal Authorities and Guidance

## Legislation

- Clinger-Cohen Act of 1996, P.L. 104-106
- Government Paperwork Elimination Act, P.L. 105-277, Title XVII
- Title 49, Transportation, as amended, 49 U.S.C. §§ 106, 40110, 40121

## DOT Policies

- DOT Order 1351.1, IT Directives Management

## Guidance

- 25 Point Implementation Plan to Reform Federal Information Technology Management, December 9, 2010
- Federal IT Shared Services Strategy Implementation Guide
- A Common Approach to Federal Enterprise Architecture, May 2, 2012
- OMB Circular A-130, Transmittal Memorandum #4, “Management of Federal Information Resources”
- OMB Memorandum M-11-29, Chief Information Officer Authorities
- Federal Information Technology Shared Services Strategy, May 2, 2012