CIOP CHAPTER 1351.28

Departmental Records Management Policy

TABLE OF CONTENTS

Table of Contents

Section 28.1 Purpose

This policy establishes the U.S. Department of Transportation (DOT) policy and assigns the responsibilities for carrying out records management requirements of the Federal Records Act[1], National Archives and Records Administration (NARA) Regulations, and the Presidential Directive on Records Management[2], as well as general records management at DOT.

This policy provides an overall, high-level direction to Components[3] for implementation and ongoing operation of an effective Records Management program at the Department and Component levels while allowing flexibility for establishment and implementation of local procedures and processes to meet specific needs of Component-level directorates, mission programs, and offices.

[1] The Federal Records Act of 1950, as amended, 44 U.S.C. Chapter 31

[2] Managing Government Records Directive, M-12-18

[3] The term "Component" refers to all DOT Operating Administrations and Secretarial Offices collectively.

Records Management program requirements outlined in this policy are designed to consistently manage government information[4] documenting key agency decisions and events. Recordkeeping requirements applied to Federal records will prevent loss of institutional knowledge by directing DOT personnel[5] to consider the effects of decisions and actions on each stage of the records lifecycle.

The accuracy and consistency of how this information is identified, captured, stored and retrieved provides the cornerstone to the effective functioning and transparent operation of the Department, and will facilitate access to information by DOT staff, stakeholders and the public.

Table of Contents

Section 28.2 Background

The term "records" as used in this policy, unless otherwise stated, refers to Federal records as defined in 44 U.S.C. 3301. This includes all recorded information[6], regardless of form or characteristic, made or received by a Federal agency under Federal law and deemed appropriate for preservation by DOT. A record evidences functions, policies, decisions, procedures, operations or other activities of the DOT.

Not all information received, created, or compiled by DOT qualifies as a Federal record. The Department is responsible for establishing effective controls over all records and nonrecord materials in its custody.

Records are the foundation of open government, supporting the principles of transparency, participation, and collaboration. Well-managed records can be used to assess the impact of programs, to improve business processes, and to share knowledge across the Department and Government. Records protect the rights and interests of people and hold officials accountable for their actions. Permanent records, as appraised and preserved by NARA, document our Nation's history.[7]

A record contributes to the narrative of the Federal Government by planning for administrative and program needs, providing evidence of DOT activities, protecting legal and financial rights, enabling oversight by Congress and other authorized agencies, documenting DOT history, and continuing key functions and activities in the event of an emergency or disaster. Records capture institutional memory, preserve the historical record, and are of critical importance in ensuring that the organization continues to function effectively and efficiently.

---

[4] For the purposes of this policy, "government information" also includes any information considered to be classified national security information.

[5] Throughout this document, the term "personnel" is used to refer to all paid and unpaid members of the DOT staff, to include contractors and subcontractors. When used in this document, the term "contractor" refers to the organization, its employees, and the five types of contractors defined by OMB: service providers; contractor support; Government Owned, Contractor Operated facilities (GOCO); laboratories and research centers; and management and operating contracts. For more details regarding contractors, see OMB Memorandum M-14-04.

[6] The term "recorded information" includes all traditional forms of records, regardless of physical form or characteristic, including information created, manipulated, communicated, or stored in digital or electronic form.

[7] OMB Memorandum M-12-18: Managing Government Records Directive

The Federal Records Act requires each Federal agency to establish a records management program: a planned, coordinated set of policies, procedures and activities needed to manage recorded information. Essential elements include issuing up-to-date records policies; properly training those responsible for implementation; and carefully evaluating the program to ensure adequacy, effectiveness and efficiency.

On November 28, 2011, President Obama signed the Presidential Memorandum—Managing Government Records. The Acting Director of the Office of Management and Budget (OMB) and the Archivist of the United States subsequently issued the Managing Government Records Directive (PRMD). This memorandum aims to modernize Federal records management by outlining steps that agencies must take in order to shift from paper to electronic records, with the aim of reducing costs in the long term and increasing transparency. Two central goals are key to this reform: Requiring electronic recordkeeping to ensure transparency, efficiency, and accountability; and demonstrating compliance with Federal records management statues and regulations.

The PRMD requires that agencies commit to more effectively manage all records consistent with Federal statutes and regulations, as well as professional standards. This includes designating and reconfirming a Senior Agency Official (SAO) for Records Management; ensuring that permanent records are identified for transfer and reported to NARA; ensuring that Component records officers (ROs) obtain NARA certificates of Federal Records Management Training; establishing RM training; and ensuring that records are scheduled.

This policy establishes a DOT records program that manages the transition of agency paper records to electronic records in the move towards digital government.

Records Lifecycle

Proper recordkeeping ensures protection from record creation through final disposition. A document that is identified as a Federal record is placed under records management control and emphasizes the entire lifecycle, rather than just creation or disposition.

Creation

Records may be information created or received by a user. Properly distinguishing records from nonrecords in the beginning of the lifecycle decreases the volume of records to be manipulated, controlled, stored, and disposed of. A proper creation process enhances the usability and value of records throughout the lifecycle.

Active Use and Maintenance

Active use refers to the point of the lifecycle when a record is accessed regularly for business use. Records management roles during the active use phase of a records life cycle are those that help ensure or facilitate ease of access to records for ongoing business uses.

Maintenance refers to the management of information. This can include filing, retrieval, and off-site storage or transfers. While filing may imply the placing of information in a prescribed container and leaving it there, filing is actually the process of arranging information in a predetermined sequence and creating a process to manage it for useful existence within an organization. This information is combined and in a central document known as a “file plan.” Failure to establish a sound file plan makes record retrieval and use difficult.

Inactive (or Semi-Active) Use

The terms "Inactive" or "Semi-Active" refer to the point of the lifecycle after records have fulfilled their active usefulness, or are only occasionally sought for reference purposes. During the inactive phase records remain in the custody of the Agency and must continue to be accessible.

Disposition

Disposition refers to the end of the record's life. After temporary records have fulfilled their NARA-approved retention periods they are destroyed or deleted,[8] while permanent records are transferred to the legal custody of the National Archives.[9]

Disposition of records should occur on a systematic and routine basis. No disposition action should take place without the assurance that the record is no longer required and that no litigation, investigation, or other matter is current or pending that would involve relying on the record as evidence.

Table of Contents

Section 28.3 Scope and Applicability

This policy applies to all DOT personnel and Components. The Office of the Inspector General (OIG) is not a DOT Component as defined in this policy, but may issue internal policies consistent with this policy and may work with the DOT Records Management Officer, when consistent with OIG independence.

This policy applies to the Federal Aviation Administration (FAA) only to the extent that such requirements and recommendations are consistent with the language contained in the FAA authorization statutes, FAA General Procurement Authority, and FAA Air Traffic Control Modernization Reviews.[10]

The Records Management Program promotes standard processes, procedures, practices and guidelines that ensure the proper handling of DOT records in accordance with applicable law and NARA guidelines. Adherence to this policy will ensure that all DOT records are maintained in accordance with Federal laws, standard business practices, and all regulatory requirements. Each DOT Component may issue additional policies and guidance provided they are consistent with existing laws, regulations, and DOT policies and procedures. This policy media- and location-neutral, applying to all records produced in the DOT, regardless of form, format, or location.[11]

---

[8] A temporary record is any record that has been determined by the Archivist of the United States to have insufficient value (on the basis of current standards) to warrant its permanent preservation by the National Archives.

[9] A permanent record is any Federal record of such historical significance as to warrant NARA's authorization of its preservation in the National Archives beyond the time that it is needed for DOT administrative, legal, or fiscal purposes.

[10] 49 U.S.C. §§ 106, 40110, 40121

[11] In addition to managing Federal records, the Department is responsible for managing records that fall outside of the Federal Records Act, commonly referred to as "nonrecords." In this policy the term "records" is used to refer to both Federal records and nonrecords. As necessary, the OCIO will address

Table of Contents

Section 28.4 Policy

DOT recognizes the importance of its records to the mission of the Department and the history of the Federal government. DOT has a responsibility to proactively manage those records in accordance with Federal law, which requires integrating records management across all DOT programs from the beginning stages of development. DOT has established a records management policy based on Federal requirements and principles adapted from commonly accepted principles of the records management (RM) community.

Special considerations must be taken into account to ensure that electronic records are managed using the same principles required for traditional media. Due to the increasing reliance on electronic records, this policy establishes standards for DOT electronic records management that encompasses records created from social media and email.

This policy will be applied in conjunction with other Departmental information management policies including, but not limited to, the Cybersecurity (DOT Order 1351.37) and Privacy Risk Management (DOT Order 1351.18) policies.[12] DOT personnel should engage with Component records management officers and other subject matter experts to address specific inquiries.

28.4.1 **Accountability and Transparency**

The DOT is committed to maintaining government records in an open and verifiable manner and making documentation available to all personnel and appropriate interested parties, consistent with Federal laws protecting particular types of information, such as trade secrets or privacy-related information. Records management programs must have a designated program structure that includes an assigned senior official to oversee program development and implementation across the Department. This ensures that the administration, governance and implementation responsibilities of the records management program are upheld. Records within DOT will support accountability by providing information about Departmental activities.

28.4.1.1 DOT will ensure that records are managed in approved records systems in accordance with Federal requirements.

28.4.1.2 DOT will establish and implement a Departmental Records Management Program that ensures dedicated management of records from their initial creation to their final disposition.

28.4.1.3 DOT will, in accordance with the PRMD, designate a Senior Agency Official (SAO) and reaffirm this designation by November 15 of each subsequent year.

28.4.1.4 DOT will accurately and completely record the activities undertaken to implement records management programs.

---

the specific application of this policy to Federal records and nonrecords in its implementation instructions and other guidance.

[12] All CIO IT Policy (CIOP) and implementation instruction may be found on the CIOP Sharepoint site - http://our.dot.gov/team/dot.it/SitePages/ciop.aspx. In addition, the policies may be found on the Department's public-facing website, https://www.transportation.gov/digitalstrategy/policyarchive

28.4.1.5 DOT will ensure adequate and proper documentation of business activities.

28.4.1.6 DOT will establish recordkeeping requirements in accordance with Federal statute.[13]

28.4.1.7 DOT will establish training for DOT personnel.

28.4.1.8 DOT will conduct assessments of its records management program and report its findings in accordance with government oversight authorities.

28.4.1.9 DOT records management policy will work in conjunction with existing DOT CIO Policy.

28.4.2 **Integrity and Protection**

DOT must ensure the authenticity and integrity of its records to provide adequate evidence and documentation of DOT business. A key factor in records management program integrity is protection, which must apply to both paper and electronic records from the moment they are created through final disposition. While DOT is committed to allowing public access to DOT information, DOT also has the responsibility for maintaining the confidentiality of certain types of information for which public disclosure is prohibited by law, such as classified national security or trade secrets. DOT records contain a variety of sensitive information and must be marked and controlled consistent with applicable policy.[14]

28.4.2.1 DOT will establish guidance in accordance with existing DOT CIO Policy to ensure that records are appropriately protected and have consistent governance throughout the records life cycle.

28.4.2.2 DOT will establish requirements to ensure that records remain in DOT custody, to the extent required by law. Removal of records from the Department's custody must be authorized by the SAO or designee.[15]

28.4.2.3 DOT will establish guidance to ensure that information systems containing records reliably uphold the integrity of the content.

Essential Records

Special protection applies to records that are critical to the Continuity of Operations Plan (COOP).[16] Because every organization is vulnerable to loss of records, all Components must have a comprehensive program for protecting essential records from catastrophe or disaster. Operated as part of the overall records management program, essential records programs preserve the integrity and confidentiality of the most important records and safeguard essential

[13] 36 CFR Part 1222

[14] For additional information on Departmental requirements for marking and controlling sensitive information, contact the Office of Security, Intelligence, and Emergency Response (S-60).

[15] "Employees with telework agreements are allowed to remove working copies. A working copy is considered to be one of the following: a preliminary form of a possible future document; a document possessing short-term or transitory value, and not considered the official record; or a reference copy."

[16] The COOP documents the overarching strategy, policies, and procedures required to support a continuity of operations program.

information assets. A plan for these records enables agency officials to identify and protect the most important records dealing with the legal and financial rights of the agency and of persons directly affected by the agency's actions.

28.4.2.4 DOT will create and maintain an essential records program that establishes standards and requirements for identifying records necessary to the Agency's continuing operations, to be included in the COOP.

28.4.2.5 Essential records will identify and protect records that specify how an agency will operate in an emergency or disaster.

28.4.2.6 Essential records will identify records needed to protect the legal and financial rights of the Government and citizens.

28.4.2.7 Essential records will remain adequately protected, accessible and immediately usable.

28.4.2.8 DOT will maintain an inventory that includes the location of essential records.

28.4.3 **Availability**

A successful and responsible organization must have the ability to identify, locate and retrieve the records required to support its ongoing business activities, and records must be separated and easily distinguished from nonrecord materials. Applying descriptive metadata to records and creating a well-designed storage process simplifies search and allows for quick retrieval.

28.4.3.1 DOT will establish requirements to ensure that records are retrievable throughout the records lifecycle.

28.4.3.2 DOT will establish requirements for consistent descriptive metadata of records.

28.4.3.3 DOT will account for all records by maintaining a complete and current inventory of records, to include records in offsite storage.

28.4.3.4 DOT will account for those records in off-site storage.[17]

28.4.3.5 DOT will create and distribute guidance establishing minimum requirements for file plans and ensure that file plans are disseminated to records owners with instructions for use.

28.4.4 **Retention and Disposition**

Retention

Proper retention ensures that records are kept in accordance with legal, regulatory, fiscal, operational and/or historical needs. As the oversight authority, all retention schedules must be approved by NARA.

Retention, or "disposition," schedules ensure that records are not held longer than necessary. Records that are kept beyond their retention times take up unnecessary space and can be costly to maintain. Maintaining records beyond their disposition date can potentially lead to review of

[17] Records that are stored off premises are maintained in a facility compliant with Federal standards. 36 CFR Part 1234, Subpart B.

outdated or irrelevant information to respond to litigation, Freedom of Information Act (FOIA), or other requests for records, resulting in an undue burden on DOT personnel.

In order to minimize risks and costs associated with retention, it is essential to dispose of records as soon as practicable after their retention period expires, unless a business or legal need requires longer retention. The ability to properly and consistently retain and dispose of information is especially important as DOT creates and stores enormous quantities of information, increasingly in electronic form.

28.4.4.1 DOT will ensure that all records are managed in accordance with NARA-approved schedules.

28.4.4.1.1 DOT will schedule records using the following order of precedence of approved schedules:

- NARA-issued General Records Schedule (GRS)
- Department-wide schedules
- Component schedules
- System/record set-specific schedules

28.4.4.1.2 DOT will ensure new records schedules are created for records not covered by a NARA-approved schedule.

28.4.4.2 DOT will manage records as permanent until NARA authorizes their disposition through an approved records schedule.

28.4.4.3 Consistent with the Department's Privacy and Risk Management Policy, record schedules for Privacy Act records limit the retention of personally identifiable information (PII) to that which is necessary to fulfill the purposes for which it is collected.

Disposition

Disposition is authorized at the end of the records lifecycle. Records eligible for disposition are those that are no longer required to be maintained by applicable laws and approved record schedules. At the completion of their retention period, records must be designated for disposition absent a records hold. In many cases, the appropriate disposition is destruction.

28.4.4.4 DOT will ensure proper disposition of records after the inactive/retention period phase is complete and records have fulfilled their prescribed retention period.

28.4.4.4.1 DOT will identify all permanent records for transfer in accordance with NARA standards and schedules.

28.4.4.4.2 DOT will ensure that records identified as permanent and that have been in existence for 30 years or more will be transferred to NARA.

28.4.4.4.3 DOT will ensure that temporary records are destroyed, deleted, transferred or donated[18] in accordance with NARA standards and schedules.

[18] 36 CFR 1226.26

Records Holds

A records hold is an authorized issuance requiring the suspension of established records retention and disposition requirements and that preserves, or "freezes," any records destruction until the hold is lifted. Record holds may be issued when litigation is reasonably expected or is in process and are also issued to retain records needed to reply to FOIA, Congressional, OIG, GAO, or other oversight requests.

28.4.4.5 DOT will suspend disposition of any records under a record hold until the hold is lifted.

28.4.4.5.1 DOT will notify affected personnel when a hold is issued and when it is released.

28.4.4.5.2 DOT will maintain an accurate accounting of all records holds and their status.

28.4.5 **Electronic Records**

As DOT adopts new electronic technologies, special attention must be paid to ensure that records management requirements and principles are incorporated within those systems.

28.4.5.1 DOT will maintain all electronic records electronically by December 31, 2019, in authorized records systems.

28.4.5.1.1 Authorized recordkeeping systems will meet requirements established by NARA.

28.4.5.2 DOT will integrate records management and preservation considerations into the design, development, enhancement, operation, and decommissioning of electronic information systems, to include, but not limited to, the following requirements:

28.4.5.2.1 Protecting against unauthorized addition, deletion, alteration, use, and concealment throughout the records management lifecycle.

28.4.5.2.2 Ensuring that records can be located, retrieved, presented, accessed and interpreted by all authorized personnel.

28.4.5.2.3 Identifying the organizational, functional and operational function of the record.

Electronic Mail and Messages

The Federal Records Act defines electronic messages as "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals."[19] Specific records management requirements apply to electronic messages.

28.4.5.3 DOT will manage all electronic messages in an accessible format.

28.4.5.3.1 All email records will be managed in an accessible electronic format by December 31, 2016.

[19] 44 U.S.C. § 2911(c)(1)

28.4.5.3.2 The Department will manage electronic messages in accordance with NARA's General Records Schedule (GRS) 6.1: Email Managed Under a Capstone Approach (Capstone Approach).

28.4.6 **Nonrecords**

For the purposes of this Policy, a nonrecord refers to Federal Government-owned documentary materials excluded from the legal definition of the records, copies, or personal papers. Nonrecords must be managed and disposed of, but are not subject to the same regulations as records. However, Government-owned nonrecord information, regardless of records status, may be subject to record holds or production requests (such as FOIA- or litigation-related requests).

28.4.6.1 DOT will establish requirements to ensure that nonrecords remain separated and easily differentiated from records.

28.4.6.1.1 DOT will establish requirements to ensure that personal papers are differentiated from government-owned information.

28.4.6.2 DOT will apply record holds to nonrecord information in accordance with this policy.

28.4.6.3 DOT will establish requirements to ensure that Government-owned nonrecords are destroyed when no longer needed for reference.

Table of Contents

Section 28.5 Roles and Responsibilities

This section defines the roles key to implementing the Departmental Records Management Program and records management-specific responsibilities associated with each role. Provided below is a listing of the roles and the levels in the organization where they reside. The Departmental Records Management Officer is the designated primary operational officer. Through the IT Governance process the Chief Technology Officer and the Chief Information Security Officer will be advocates for proper records management as outlined in this policy. The DOT's records management program is overseen by the Chief Information Officer (CIO), who serves as the Senior Agency Official for Records Management (SAORM).

Department Level

- Departmental Chief Information Officer
- Departmental Associate Chief Information Officer for IT Policy and Oversight
- Departmental Records Management Officer
- Departmental Chief Security Officer
- Departmental Chief Privacy Officer
- Office of the General Counsel
- Office of the Senior Procurement Executive

Component Level

- Component Officer Responsible for Records Management
- Component Records Management Officer
- Component Chief Information Officer

- Component Information Systems Security Manager(s)
- Component Privacy Officer
- Component Chief Counsel

Program Level

- Record Owner
- Business Owner
- Contracting Officer
- System Owners

DOT Personnel

- All DOT Employees and Contractors

Department Level

28.5.1 Accountability for directing DOT's information and data integrity, and for all IT functions, resides with the **DOT Chief Information Officer (CIO)**. In addition to responsibilities listed elsewhere in Departmental policy, the DOT CIO serves as the Departmental SAORM, as required in the PRMD. The DOT CIO will:

28.5.1.1 Appoint a Departmental Records Management Officer (DRMO), certified to NARA standards, to assist with implementation, evaluation and administration issues regarding the Federal Records Act PRMD and applicable legislation.

28.5.1.2 Ensure a Departmental Records Management Program is developed, documented, implemented and promoted to support records management activities for all information systems, networks and data that support Departmental operations.

28.5.1.3 Maintain a central policy-making role in the organization's development and evaluation of legislative, regulatory and related policy proposals involving records management issues.

28.5.1.4 Ensure the organization establishes and implements records management, including full compliance with Federal laws, regulations and policies relating to records management.

28.5.1.5 Ensure records management processes are integrated with DOT strategic and operational planning processes.

28.5.1.6 Provide resources to administer the Departmental Records Management Program.

28.5.2 Oversight and advocacy of the Departmental Records Management Program is designated to the office of IT Policy and Oversight. The **Departmental Associate Chief Information Officer for IT Policy and Oversight** will:

28.5.2.1 Ensure the Departmental Records Management Program is appropriately staffed and resourced.

28.5.2.2 Assume all operational oversight and strategic direction responsibilities for the records management program as delegated by the SAORM.

28.5.2.3 Approve the Department's submission of records management reporting activities in coordination with input from Department and Component officials, as applicable.

28.5.2.4 Integrate Records Management into the Departmental Governance and Oversight framework.

28.5.2.5 Ensure that new or reorganized DOT Components, programs and projects incorporate recordkeeping requirements as an active decision-making factor in all systems.

28.5.3 Operationalization of the Department Records Management Program is assigned to the **Departmental Records Management Officer** (**DRMO)**. The DRMO will:

28.5.3.1 Create and manage the Department-wide records management program as the lead records management officer for inter-agency initiatives.

28.5.3.2 Establish the framework for the records management program to ensure that the Department meets operational, legal and regulatory requirements.

28.5.3.3 Assist in the planning and implementation of information technology and reviewing the purchase of records management equipment and electronic records management solutions to ensure they conform to Federal statutory and regulatory requirements.

28.5.3.4 Lead, plan and manage the Department's records management program for both core mission and administrative records, regardless of medium or format.

28.5.3.5 Provide technical support and guidance for the development, integration and promulgation of policy and procedural requirements covering records management on such areas as systems security, quality assurance, training and lifecycle management.

28.5.3.6 Ensure, in consultation with senior program managers and officials, that data and information provided in response to audits and reviews are accurate and complete to the extent possible.

28.5.3.7 Create and maintain DOT-wide Records Retention and Disposition Schedules for common DOT records to instruct programs on how long to maintain records with similar functions.

28.5.3.8 Coordinate with Component Records Management Officers to review proposed schedules prior to submission to NARA.

28.5.3.9 Provide guidance and oversight to Components regarding implementation of the essential records program.

28.5.3.10 Establish and disseminate standards to ensure that Components clearly identify staff responsibilities to comply with an essential records management program.

28.5.3.11 Establish and assess records management practices to ensure they support the principles of transparency and information sharing throughout DOT.

28.5.4 The **Departmental Chief Information Security Officer (DOT CISO)** is responsible for establishing and maintaining the DOT vision, strategy and program to ensure information assets and technologies are adequately protected. The CISO will work with the DRMO to:

28.5.4.1 Ensure that all official records management systems are certified and accredited in accordance with Federal requirements and Departmental Order 1351.37, Departmental Cyber Security Policy.

28.5.4.1.1 Ensure that records are maintained in a manner that prevents loss, theft, misuse, or unauthorized access or alteration throughout the record lifecycle.

28.5.4.1.2 Establish assessment standards and processes for records management-related cybersecurity controls.

28.5.5 The **Departmental Chief Privacy Officer (DOT CPO)** is responsible for ensuring that the Department limits the retention of personally identifiable information (PII) that is necessary to fulfill the purpose of collection. The DOT CPO will:

28.5.5.1 Ensure that the Department retains collections of PII only as long as necessary to fulfil the purposes of the collection as:

- Identified in notice provided to the individual at the time of collection
- Required by law

28.5.5.2 Coordinate with the DRMO, NARA, and Component officials to identify appropriate retention periods for records subject to the Privacy Act prior to the submission of any retention schedule to NARA for approval.

28.5.5.2.1 Ensure that the retention discussion in all Departmental Privacy Act notices is consistent with the NARA-approved records schedule for the system of records.

28.5.5.3 Ensure that the Department disposes, destroys, erases, and/or anonymizes PII, in accordance with NARA-approved record retention schedules, including PII maintained in:

- Originals,
- Copies, and
- Archived records.

28.5.6 The DOT **Office of the General Counsel (OGC)** is the office of the chief legal officer of the Department, legal advisor to the Secretary, and final authority on questions of law within the DOT. The OGC will consult with the DRMO to:

28.5.6.1 Issue notification and requirements of legal record holds for documents housed within OST (and where appropriate, Components, if they house related documents) necessitated by litigation, investigations, or other matters.

28.5.6.2 Provide legal advice and counsel on all matters arising in the administration of this policy.

28.5.7 The DOT **Office of the Senior Procurement Executive (SPE)** facilitates the accomplishment of DOT's mission by providing policies, practices and services regarding acquisition, financial assistance management and competitive sourcing. The SPE will:

28.5.7.1 Partner with the DRMO to develop and implement DOT-specific records management-related contract clauses for incorporation in all current and future contracts and covered grants, and promote their use.

28.5.7.2 Ensure contracting officers (COs) include the requirements of record management clauses, including NARA guidance on contract language. [20]

[20] http://www.archives.gov/records-mgmt/handbook/records-mgmt-language.html

28.5.7.3 Include appropriate records management requirements in all contracts and other acquisition-related documents for DOT information systems developed, maintained, operated, or managed by contractors.

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

Component Level

28.5.8 Accountability for directing records management varies by Component. Each DOT Component may locate its Records program under the CIO or elsewhere in the organization. Regardless of organizational alignment, the **Designated Office of Responsibility** will:

28.5.8.1 Ensure that records officers are certified in accordance with PRMD and NARA within one year of assumption of position.

28.5.8.1.1 If records officers are not certified within one year, ensure that they have a letter of exemption from NARA.

28.5.8.2 Designate a point of contact for the management of essential records and implementation of the essential records management program within the Component.

28.5.8.3 Ensure the Component records management office is appropriately staffed and resourced.

28.5.9 The **Component Records Management Officer (RMO)** serves as the primary point of contact for Component records management concerns and implementation of the Component records management program. The RMO, or his/her designee will:

28.5.9.1 Support Departmental efforts to develop a records management program;

28.5.9.1.1 Participate and contribute to Departmental Records Officers efforts to establish common process, procedures and capabilities.

28.5.9.1.2 Implement Departmental standards and practices.

28.5.9.2 Serve as the primary official for assisting the Component in implementing a records management life cycle program and this policy.

28.5.9.2.1 Develop and implement Component procedures, records retention schedules, guidance, and other records management tools consistent with Departmental and NARA guidance and policy.

28.5.9.3 Ensure that records are managed appropriately and are accessible throughout their life cycle. The RMO will work with records owners to:

28.5.9.3.1 Create and maintain an accurate records inventory.

28.5.9.3.2 Develop a file plan that specifies how records are to be organized once created or received.

28.5.9.3.3 Administer processes for developing and submitting new or revised retention schedules for approval by the Archivist of the United States.

28.5.9.3.3.1 Notify the Component Privacy Officer of any records collection containing PII and work to ensure that the retention of such records is the minimum necessary.

28.5.9.3.4 Apply the appropriate disposition to all records regardless of location and notify the appropriate program office and the off-site facility, as necessary, of changes in disposition authority due to updated records disposition schedules.

28.5.9.3.5 Oversee and coordinate records transfers and dispositions including establishing and monitoring agreements/contracts.

28.5.9.3.6 Ensure that records are not removed outside of DOT facilities unless expressly approved in writing.

28.5.9.3.7 Ensure the legal destruction of eligible Component records and the transfer of permanent records to the legal custody of NARA.

28.5.9.4 Perform audits and ensure compliance of agency recordkeeping practices with existing statutes and internal and external regulations.

28.5.9.5 Ensure that all Component personnel are meeting their responsibilities for appropriately managing records they create, receive or maintain.

28.5.10 Accountability for directing the information and data integrity of the Component and its groups resides with the Component CIO. In addition to responsibilities listed elsewhere in Departmental policy, the **Component CIO** will:

28.5.10.1 Coordinate with Component budgetary offices to ensure appropriate records management activities and documentation for IT systems and services are included as part of capital planning and investment control (CPIC) and other IT governance processes.

28.5.10.2 Ensure that Federal records in IT systems are maintained during all phases of the records lifecycle.

28.5.11 The records-management related responsibilities of **Component Information Systems Security Managers (ISSM)** or equivalent designees include, but are not limited to;

28.5.11.1 Working with the Component Records Management Office to ensure that authorized electronic records keeping systems are appropriately certified and accredited

28.5.11.1.1 Ensuring that electronic records are appropriately secured throughout their lifecycle.

28.5.11.1.2 Ensuring that authorized records schedules are accurately implemented in the electronic recordkeeping systems.

28.5.12 The **Component Privacy Officer's r**ecords management responsibilities include, but are not limited to;

28.5.12.1 Ensuring that records include the minimum necessary collection of Personally Identifiable Information (PII) and to that which is necessary to execute an authorized purpose of the Department.

28.5.12.2 Working with Component Records Officers to minimize the retention periods for records subject to the Privacy Act prior to the submission of any retention schedule to NARA for approval.

28.5.12.2.1 Ensure that the retention discussion in all Component Privacy Act notices is consistent with the NARA-approved records schedule for the system of records.

28.5.13 The **Component Chief Counsel** is the legal advisor to the Component Administrator and will work with the Component RMO and other Component and Departmental officials to:

28.5.13.1 Issue notification and requirements of legal record holds housed within the Component necessitated by litigation, investigations, or other matters.

28.5.13.2 Provide legal advice and counsel on all matters arising in the administration of this policy.

Program Level

28.5.14 A **Records Owner (RO)** is the individual who understands a specific record system and is responsible for making decisions on retention and disposition of the records. **Records Owners** will:

28.5.14.1 Ensure that system records are listed in the Departmental file plan and are described accurately.

28.5.14.2 Work with the Component RO on records identification, preservation and disposal.

28.5.15 A Business Owner is the champion of and owner of the requirements for the service, activity, or information system and its associated records. **Business Owners** will:

28.5.15.1 Ensure resources are appropriately requested and applied to meet records management standards.

28.5.15.2 Communicate business requirements for records created under the applicable service, activity, or system.

28.5.15.2.1 Collaborate with Component RMO to establish minimum retention requirements.

28.5.15.3 Ensure business program records are managed in accordance with approved NARA record schedules.

28.5.15.4 Notify the Component RMO when establishing, revising, or deleting an information system that contains records.

28.5.16 The Contracting Officer (CO) has the authority to enter into, administer and/or terminate contracts, and make related determinations and findings. The **CO** or **CO's Representative (COR)** will:

28.5.16.1 Coordinate with the System Owners, Business Owners, Project Officers/Managers and Component RMOs to ensure that the appropriate records management language is incorporated into all contracts and upheld.

28.5.16.2 Advise contractors that develop or maintain a system that manages records on behalf of the Federal Government that the Federal Records Act applies to them to the same extent that it applies to Federal staff, per the Federal Records Act.

28.5.17 The System Owner or System Manager is the key point of contact (POC) for the information system and is responsible for coordinating System Development Life Cycle activities specific to the information system. **System Owners** will:

28.5.17.1 Incorporate DOT and Component guidance for records management functions into the design, development, and implementation of information systems.

Personnel

28.5.18 DOT personnel are all members of the DOT staff, including contractors and subcontractors. All **DOT Personnel** will:

28.5.18.1 Ensure the safekeeping of Federal government records by managing them in accordance with this Policy.

28.5.18.2 Use official electronic messaging systems to conduct DOT business.

28.5.18.2.1 In the event that DOT business is authorized be conducted using non-official electronic messaging system:

28.5.18.2.1.1 Copy an official electronic messaging account of the officer or employee in the original creation or transmission of the record; or

28.5.18.2.1.2 Forward a complete copy of the record to an official electronic messaging account of the officer or employee not later than 20 days after the original creation or transmission of the record.

28.5.18.3 Complete Department-provided records management training within 90 days of hire and every two years thereafter.

28.5.18.4 Report all suspected and actual unauthorized destruction of Federal records to the Component Records Management Officer.

Table of Contents

Section 28.6 Dates

28.6.1 The effective date of this policy is the date the policy is signed.

28.6.1.1 The DOT will meet all reporting deadlines consistent with the most recent OMB Records Management guidance.

28.6.1.2 The DOT will reaffirm the SAO by November 15th of each year.

28.6.1.3 In accordance with the CIOP and the DOT Order Directive Process, this chapter will be reviewed annually and validated by the DOT CIO. The policy content will be annually reviewed to ensure it has clear intent, contains the correct material and complies with the IT Directive Publication Process. Roles and responsibilities will be reviewed and updated on a quarterly basis

Table of Contents

Section 28.7 Cancellations

28.7.1 This policy supersedes the following previously issued policy and guidance:

28.7.1.1 CIOP Chapter 1351.28, dated November 2010.

Table of Contents

Section 28.8 Compliance

28.8.1. The DOT Components must comply with and support the implementation of a Departmental Records Management Program, to include compliance with Federal requirements and programmatic policies, and procedures.

28.8.2. 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).

28.8.3. This policy does not supersede any other applicable law, higher-level Agency policy, or existing labor management agreement in place as of the effective date of this policy.

28.8.4. Departmental officials must apply this Departmental Records Management Policy to employees, contractor personnel, interns, and other non-governmental employees.

28.8.5. All DOT Components collecting or maintaining information or using or operating information systems on behalf of the Department are also subject to this Departmental Records Management Policy.

28.8.6. The content of this Departmental Records Management Policy must be incorporated into applicable contract language as appropriate.

28.8.7. Any person who improperly destroys, conceals, or removes any Federal records is subject to penalties under 18 U.S.C. 2071.

28.8.8. Compliance with this policy is mandatory.

28.8.9. DRMO will conduct periodic evaluations of this policy and of records management programs throughout the Department to ensure compliance with this policy.

Table of Contents

Section 28.9 Waivers

28.9.1. The DOT Components may request that the DOT CIO/SAORM 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) what measures have been implemented to ensure that records management principles have been implemented (3) waiver period and (4) milestones to achieve compliance. The DOT CIO/SAORM will provide a written waiver or justification for denial.

Table of Contents

Section 28.10 Audit Procedures

28.10.1 In order to ensure the Department provides appropriate accountability for records management, and that the DRMO provides active support and oversight of monitoring and improvement of the Departmental Records Management Program, the DRMO must:

28.10.1.1 Develop and implement an oversight and compliance function to provide the required guidance and reviews to meet the Federal Records Act and the Presidential Records

Management Directive and other Department-and Federal Government wide services management requirements;

28.10.1.2 Conduct annual compliance reviews of DOT Records Management Programs;

28.10.1.3 Develop and manage the Departmental Records Management Program, reporting progress to the DOT CIO and Secretary of Transportation;

28.10.1.4 Monitor Component efforts to identify and address weaknesses in their respective records management programs;

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

28.10.1.6 Conduct an audit of the DOT Records Management Policy program, as required by 1351.1 IT Directives Management, as amended.

Table of Contents

Section 28.11 Approval

X RICHARD MCKINNEY

Digitally signed by RICHARD MCKINNEY
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=RICHARD MCKINNEY
Date: 2016.08.11 15:35:31 -04'00'

Richard McKinney
Chief Information Officer, U.S. DOT

Table of Contents

Appendix A: Definition of Terms

Accession: Transfer of legal and physical custody of Permanent Records from a Federal Agency to NARA.

Active Records: Records necessary to conduct current DOT business and therefore stored onsite or otherwise kept readily accessible, physically or electronically.

Adequate and Proper Documentation: A Record of the conduct of Federal Government business that is complete and accurate to the extent required to document the organization, functions, policies, decisions, procedures, and essential transactions of each Federal Agency and that is designed to furnish the information necessary to protect the legal and financial rights of the Federal Government and the Federal Agency, and of persons and entities directly affected by the agency's activities. *See* 36 C.F.R. § 1220.18.

Administrative Records: Records that are preserved because they facilitate the operations and management of a Federal Agency, but do not relate directly to programs that help achieve the Agency Mission. Administrative Records relate to activities such as budget and finance, human resources, equipment and supplies, facilities, and contracting.

Archivist: A NARA representative responsible for functions listed under the definition for *National Archives and Records Administration (NARA).*

Business Owner The spokesperson for the IT service initiative and the owner of the business, functional and funding requirements for the system/service throughout the business's life cycle, from concept to disposal. The business owner works with various parties depending on the life cycle phase of the business. (Source: DOT OCIO IT Governance Guidance Memo, June 2010)

Continuity of Operations Plan (COOP Plan): A written procedure setting out the measures to be taken to minimize the risks and effects of Disasters and to recover, save, and secure the Essential Records should such a Disaster occur.

Copy: (1) A reproduction of the contents of an original document prepared simultaneously or separately and usually identified by function or by method of creation. Copies identified by function include action copy, information or reference copy, official file copy, reading or chronological file copy, suspense or tickler file copy, and stock copy. Copies identified by method of creation include carbon copy, electrostatic copy, mimeograph copy, and ribbon copy.

(2) In electronic records, the action or result of reading data from a source, leaving the source data unchanged, and writing the same data elsewhere on a medium that may differ from the source medium.

Creation: The first stage of the Records Management Lifecycle in which records are made or received by an office.

Custody: Guardianship, or control of records, encompassing both physical possession (physical custody) and legal control (legal custody), unless one or the other is specified.

Deleting: Removing, erasing, scratching, or obliterating recorded information from an electronic storage medium so that the data is no longer recoverable by keystrokes, but remains forensically recoverable until it has been overwritten multiple times by other data. If the medium is reused to store other data after deleting, the new data overwrites the deleted data.

Disposition: Actions taken with regard to Federal records that are no longer needed for current government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure. Disposition is a comprehensive term that includes both destruction and transfer of Federal records to the National Archives of the United States.

Electronic Information System: An information system that contains and provides access to computerized Records and other information. *See* 36 C.F.R. § 1236.2 and § 1236.10.

Electronic Records: Electronic, or machine-readable records, are records on electronic storage media. Electronic records are any information that is recorded in a form that only a computer can process. *See* 36 C.F.R. § 1234.2

Electronic Recordkeeping: Creating, maintaining, using, and disposing of Records using an Electronic Recordkeeping System.

Federal Records: Records subject to the Federal Records Act and include records that document the persons, places, things, or matters dealt with by the agency; facilitate action by agency officials and their successors in office; encourage Government transparency in order to facilitate scrutiny by authorized agencies of the government; protect the financial, legal, and other rights of the government and of persons directly affected by the government's actions; document the formulation and execution of basic policies and decisions and the taking of necessary actions, including all substantive decision and commitments reached orally or electronically; or document important board, committee or staff meetings.

File Plan: A classification scheme that sets out the description, arrangement, storage, retrieval, and ownership of Hard Copy Records and Electronic Records.

General Records Schedule (GRS): Records Retention Schedules issued by the Archivist of the United States to provide Disposition Authority for Records common to several or all Federal Agencies (including Records relating to personnel, fiscal accounting, procurement, communications, and other common functions).

Inactive Records: Records that are at the end of a business process, not in frequent use, and/or are not required for current DOT business.

Inventory: A list or survey of DOT Records and Non-records that is created or conducted to, among other things, identify Unscheduled Records, develop Records Retention Schedules, collect Records Management information, and obtain statistical information like volume, usage, date range, location, and medium.

Legal Hold: A communication issued as a result of current or reasonably anticipated litigation, audit, Federal Government investigation, Congressional inquiry, FOIA request, Privacy Act request, or other such matter that suspends the normal disposition or processing of records or nonrecords.

Metadata: Elements that provide administrative, descriptive, and technical information that describe the structure and content of electronic records. Metadata elements also provide contextual information that explains how electronic records were created, used, managed, and maintained prior to their transfer to NARA, and how they are related to other records.

National Archives and Records Administration (NARA): The Federal Agency responsible for appraising, accessioning, preserving, and making available Permanent Records and for issuing disposition authority for Temporary Records.

Non-records: Federal Government-owned documentary materials that do not meet the definition of Records. These include stocks of publications; library and museum material made or acquired and preserved solely for reference or exhibition purposes; duplicate copies of Records maintained solely for convenience of reference; processed or published materials; catalogues and trade journals; and papers of transitory value, such as non-circulating drafts, worksheets, informal notes and routing slips. Nonrecords can have evidentiary value and therefore may be within the scope of a Legal Hold. *See* 36 C.F.R. § 1222.14

Offsite Storage Facility: A facility external to the agency where Records, typically Inactive Records, are stored and remain searchable and retrievable pending final disposition.

Permanent Records: Records appraised by NARA as having sufficient historical or other value to warrant permanent preservation at the National Archives after they are no longer needed for DOT's administrative, legal, or fiscal purposes.

Personal Papers: Documents belonging to an employee that are not used to conduct agency business and are related solely to the employee's own affairs or used exclusively for employee's convenience.

Preserve: Ensuring Records remain available, accessible, searchable, usable, readable, and understandable through time.

Recordkeeping Requirements: All statements in statutes, regulations, rules, and Federal Agency directives or other authoritative issuances that set forth general or specific requirements for Federal Agency personnel on particular Records to be created and maintained by the agency. *See* 36 C.F.R. § 1220.18.

Records: All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them. *See* 44 U.S.C. 3301.

Records Owner:

Records Retention Schedule: An agency-specific description of Disposition Authority for records.

Retention Period: The length of time that Records must be retained by a Federal Agency before they are eligible to be destroyed, if Temporary Records, or transferred to the National Archives, if Permanent Records.

Retention Requirement: The length of time and circumstances under which a record will be retained.

Retrieval: The process by which a Federal Agency recalls Inactive Records from offsite storage.

Scheduling: The process of determining and recording the appropriate retention period and ultimate disposition of a record series. Once NARA has approved the schedule, the records are called Scheduled Records.

Temporary Records: Records for which NARA has approved a finite retention period based on the length of time the records are needed for the Federal Agency's administrative, legal, or fiscal purposes. Temporary Records do not have historical or other value warranting permanent preservation at the National Archives.

Transfer: The process of moving records from one location to another, especially from office space to off-site storage facilities, from one agency to another, or from an agency to an offsite storage location or to NARA.

Essential Records: Records essential to the continued functioning or reconstitution of a Federal Agency during and after a disaster or other emergency, and also those records essential to protecting the legal and financial rights of the relevant agency and of the individuals directly affected by its activities. Include both emergency-operating and rights-and-interests records.

Vital Records Program: Policies, plans, and procedures developed and implemented to identify, use, and protect Vital Records during and after a Disaster or other emergency.

Table of Contents

Appendix B: Legal Authorities and Guidance

Legislation

- 36 CFR Chapter XII, Subchapter B
- Federal Records Act, USC 44 Chapter 35
- The Privacy Act of 1974, as amended, 5 U.S.C. 552a
- The Paperwork Reduction Act of 1995, as amended, 44 U.S.C. 3501, et seq.
- E-Government Act of 2002, P.L. 107-347
- Freedom of Information Act of 1966, as amended, 5 U.S.C. 552
- Federal Information Security Management Act, P.L. 107-347, Title III
- Government Paperwork Elimination Act, P.L. 105-277, Title XVII

National Policy, Directives and Memoranda

- OMB Memorandum M-12-18: Managing Government Records Directive
- OMB Circular A-130: Managing Information as a Strategic Resource

DOT Policies

- U.S. Department of Transportation Information Technology Governance Policy (DOT Order 1351.39)
- U.S. Department of Transportation Cybersecurity Policy (DOT Order 1351.37)
- U.S. Department of Transportation Data Release Policy (DOT Order 1351.34)
- U.S. Department of Transportation Paperwork Reduction Act and Information Collection Policy (DOT Order 1351.29)
- U.S. Department of Transportation Web Policy (DOT Order 1351.24)

Guidance

- NARA Bulletin 2010-05 Guidance on Managing Records on Cloud Computing Environments
- NARA Bulletin 2012-02: Guidance on Managing Content on Shared Drives
- NARA Bulletin 2014-02 Guidance on Managing Social Media Records
- NARA Bulletin 2013-02 Guidance on a New Approach to Managing Email Records
- NARA Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18), April 2016

Table of Contents