July 25, 2017

The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable Tom Carper
United States Senate
Washington, DC 20510

Dear Ranking Member McCaskill and Senator Carper:

Thank you for your letter of June 8, 2017, requesting that we review the U.S. Department of Transportation’s (DOT) processes and compliance with applicable legal standards for preserving Federal electronic records, as well as DOT’s cooperation with Congressional document requests.

Your letter included six areas of inquiry related to these topics. We took a number of actions to respond to your inquiries, including reviewing documents and interviewing staff in the Office of the Secretary and researching applicable laws and guidance. In addition, we sent an email to all DOT employees through the Department’s broadcast email message system asking them to contact the Office of Inspector General (OIG) Hotline should they have information relevant to your request.1 In response to our broadcast email, we received 10 responses. Though you asked us to review actions taken by the Department and its officials since January 20, 2017, we reviewed the period since January 1, 2016. We also afforded the Department an opportunity to respond to your questions. The Deputy Secretary’s response is included as enclosure 1 to this letter. We have also attached, as referenced in the Deputy Secretary’s response, the Department’s response to inquiries from Representatives Jason Chaffetz and Elijah E. Cummings, Chairman and Ranking Member of the House Committee on Oversight and Government Reform, as enclosure 2. Enclosure 3 lists prior OIG recommendations related to your request.

Our responses to your inquiries are as follows.

1 According to the Office of the Chief Information Officer, our email message was sent to 71,064 DOT email inboxes, including employees and contractors. We also forwarded a copy of the email message to 450 OIG email inboxes.
We Found No Evidence That DOT Delays or Withholds Responses to Non-Chairman Requests for Information

We found no evidence that DOT officials have directed or advised agency employees to delay or withhold information to non-Chairmen of Congressional committees. Our detailed responses to your questions in this area are below.

1. Since January 20, 2017, has any Department official directed or advised any agency employee to delay or withhold a response to a Congressional request for information?

2. Since January 20, 2017, has any Department official directed or advised any agency employee or Congressional staff member that the agency will only provide requested documents or information to a Committee chair?

We found no evidence that any Department official directed or advised any agency employee to delay or withhold a response to a Congressional request. We also found no evidence that any Department official directed or advised any agency employee or Congressional staff member that the agency will only provide requested documents or information to a Committee chair.²

On June 20, 2017, we emailed all DOT officials and employees, including employees of all DOT Operating Administrations, providing notice of your inquiry and informing employees to contact the OIG Hotline should they be aware of any instances of instruction to delay or withhold responses to a Congressional request for information or to only provide responses to Committee chairs. The OIG Hotline did not receive any information related to the handling of Congressional requests as of July 19.

We also provided the Department an opportunity to respond to your questions. In the Department’s response, the Deputy Secretary emphasized that Secretary Chao has prioritized working with Congress “on a bipartisan basis,” including “ensuring that Congressional correspondence is responded to appropriately.” The Department’s response stated that from January 20, 2017, to June 26, 2017, DOT sent approximately 864 response letters to more than 158 members of Congress, from both parties, in both the House and Senate. The Department added that Secretary Chao has met with or spoken to Members of Congress from both parties as well. We reviewed the response letters to Congressional inquiries that the Department provided to us, and confirmed that they included examples of correspondence with non-Chairmen and Minority Members.

² The scope of our review did not include examples when laws, such as the Privacy Act (5 U.S.C. § 552a), have been interpreted as limiting the right of non-Chairmen to receive sensitive information.
In addition, we spoke to the Deputy Assistant Secretary for Congressional Affairs. His duties include managing the interaction between the Department and Congress, including managing Congressional requests. He informed us that his office has a policy of responding to all Members. He also informed us that he is not aware of any instance in which a Member’s office has complained of not receiving a response to a request.

We Did Not Find Significant Concerns Regarding the Department’s Record Retention Guidance or Use of Encryption-Capable Messaging Apps

Overall, we found that DOT has issued guidance and training in compliance with Federal law and National Archives and Records Administration (NARA) guidance pertaining to the retention of electronic records and the use of personal email and messaging accounts for conducting Government business. We also found no evidence that DOT officials or employees are using auto-deletion features on smartphone apps to conduct official business. We did find some evidence that employees may be using encryption-capable non-official messaging apps for official business. Most of the reports we received were limited to career employees using the apps primarily for minor logistical purposes. We referred one report from the time period of our review (but before the time period you asked us to review) to an Operating Administration so that it can determine whether any Federal law and/or NARA or Departmental guidance regarding electronic records preservation was not followed and take appropriate action if necessary. In the past 10 years, our office has issued three recommendations to DOT regarding electronic records retention, all of which have been closed.

Our detailed responses to your questions in this area are below.

3. Has the Department issued any guidance related to the use of smartphone applications that support encryption or the ability to automatically delete messages after they are read or sent for work-related communications?

To reduce the likelihood that work-related messages sent from non-official accounts are not properly captured and preserved, Federal law requires executive agencies to establish policies and procedures for maintaining documentation of all meetings, instant messages, phone calls, and email exchanges containing substantive information about agency activities. In addition, under Federal law, if an officer or employee of an executive agency creates or sends an electronic message regarding official business on a personal account, he or she must either (1) copy an official electronic messaging account in the original creation or

---

3 We note that DOT, like other Government agencies, issues devices such as iPhones and iPads for official Government business, which encrypt some text messages.

4 36 CFR 1222.28(d).
transmission of the record, or (2) forward a complete copy of the record to his or her official electronic messaging account not later than 20 calendar days after the original creation or transmission of the record. As with all other Federal records, the law requires that agencies must have records schedules that cover electronic messages.

DOT’s guidance regarding electronic messaging for work-related communications includes the following:

- DOT Order 1351.28 (Records Management) states that DOT personnel will use official electronic messaging systems to conduct DOT business.

- DOT Order 1351.33 (Departmental Web-based Interactive Technologies Policy) requires that any information that meets the definition of a Federal record and is disseminated electronically must be documented in an official DOT recordkeeping system and retained and disposed of, or permanently preserved, in accordance with records schedules approved by NARA.

- DOT’s records management policy further states that if DOT business is authorized to be conducted using a “non-official messaging system,” employees must copy or forward the record to their official electronic messaging account not later than 20 days after the record’s original creation or transmission. This requirement is also referenced in several guidance documents posted on the DOT intranet.

We note the following regarding DOT policy on the specific issues you have asked us to review:

- **Auto-Delete.** According to the Deputy Secretary, “tools that automatically delete messages have not been approved or endorsed for official business use.” The Deputy Secretary noted that while the Department has not issued specific guidance regarding auto-deleting apps such as Signal and Confide, any use of such apps would be subject to DOT policy.

---

7 44 U.S.C. § 3301 defines “record” as including “all recorded information, regardless of form or characteristics, made or received by a Federal agency 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 United States Government or because of the informational value of data in them.”
8 DOT Order 1351.33, Appendix A: Employee Conduct Policy. The policy defines work-related use of web-based interactive technologies to include (1) representing DOT online in an employee’s official capacity, (2) internal blogs or wikis used for collaboration among agency project teams, and (3) using external sites to engage with others in a community of practice for professional development purposes.
• **Encryption.** DOT policy does not specifically address the use of electronic messaging apps that support encryption. We identified no Federal law or NARA guidance specifically addressing encrypted text messaging apps. However, in a March 2017 memorandum to all Federal agencies, the NARA Archivist stated that the use of encrypted text messaging apps is a “high-visibility” topic that agencies must address in the coming year. The Department has advised us that it plans to review the NARA Archivist’s memorandum for applicable content and will incorporate the appropriate changes into its annual policy update later this year as well as DOT training.

Because auto-deleting messaging apps are not authorized systems and because they make it difficult or impossible to document, retain, and dispose of messages in accordance with Federal law, it would be impossible or exceedingly difficult for an employee to use such an app to conduct DOT business while complying with DOT policy and guidance.

DOT has also established records management training for its employees. DOT’s most recent training instructs employees to copy themselves or forward to an official account within 20 days when using “personal email account(s) while conducting agency business.” The training materials did not specifically address how this requirement applies to text messaging. Although recent DOT guidance makes the point that official records are “media neutral” and may include electronic forms, employees may not be aware of their record preservation responsibilities when texting with colleagues and others about official business on a personal account.

4. **Has any Department official used, for work-related communications, a smartphone app that supports encryption or the ability to automatically delete messages after they are read or sent?**

Some DOT employees have used messaging apps that support encryption. In particular, the OIG Hotline received several reports of employee use of the text messaging app WhatsApp, which supports encryption. Several reports were self-reports by employees who did not believe they were doing anything improper. Some reports we received indicated that texting via WhatsApp was a convenient means to communicate with their groups. Other than the previously mentioned

---


12 According to Office of the Chief Information Officer officials, about 90 percent of the approximately 5,600 DOT-furnished mobile devices (excluding the Federal Aviation Administration, Office of Inspector General, and U.S. Merchant Marine Academy) are iPhones and iPads. These devices come with a stock messaging app, “Messages,” that supports end-to-end encryption. See [https://www.apple.com/privacy/approach-to-privacy/](https://www.apple.com/privacy/approach-to-privacy/). According to OCIO officials, the Messages app is authorized for official use subject to DOT records management policy, namely the requirement to copy or forward a message to an official account within 20 days.
report that we referred to an Operating Administration, these reports were related
to communication about logistical rather than policy-related issues. Other reports
demonstrated confusion regarding the appropriateness of employee union
members using their union email accounts when interacting with the agency.

5. Has any Departmental official failed to abide by Federal law and/or NARA or
Departmental guidance regarding the preservation of electronic records related
to official business created on non-Government accounts?

According to Office of the Chief Information Officer officials, they are not aware
of any recent violations of law or guidance regarding preservation of electronic
records related to official business created on non-Government accounts. They
stated that to the best of their knowledge, Departmental officials and employees
are following DOT policies.

We referred one report from the OIG Hotline to an Operating Administration for
further action. The report indicated that some DOT career employees, including
one supervisor, have been communicating about an office restructuring effort at
least in part over an encryption-capable non-official messaging app. However, the
employee who filed the report became aware of communication over the
encryption-capable app in November 2016, before the time period you asked us to
review. We informed the Operating Administration of this report so that it could
take action to preserve any Government records, provide education about Federal
records laws, and, if appropriate, take administrative action. It is unclear at this
time whether official records were created and, if so, whether they were captured
in an official account within 20 days as required by law.

OIG did not initiate any investigations related to the self-reports we received,
because we did not discern an intent to evade Government records laws.

6. Has the OIG previously provided recommendations to the Department regarding
its management of the preservation of electronic records and compliance with
Congressional document requests?

OIG has issued no recommendations concerning Congressional requests for
information.

We have previously issued three recommendations to DOT in two reports relating
to management of the preservation of electronic records. Two recommendations
pertained to employees’ manual removal of data from the National Highway
Traffic Safety Administration’s (NHTSA) National Driver Register—NHTSA’s
database of individuals who have had their motor vehicle licenses suspended or
revoked. One recommendation pertained to NHTSA’s retention of pre-
investigative records when investigating vehicle defects. All three
recommendations have been closed in response to the Department’s actions. See enclosure 3 to this letter for more details.

Thank you for your attention to the Department’s compliance with Congressional requests for information and electronic records retention laws and policies. We will keep you informed on any further work that we perform in these areas, as appropriate.

If you have any questions or need further information, please contact me at (202) 366-1959 or Nathan Richmond, Director and Counsel for Congressional and External Affairs, at (202) 366-8751.

Sincerely,

Calvin L. Scovel III
Inspector General

Enclosures (3)

cc: The Honorable Ron Johnson
    Chairman
    Committee on Homeland Security and Governmental Affairs
    United States Senate
July 7, 2017

The Honorable Calvin L. Scovel III  
Inspector General  
U.S. Department of Transportation  
Suite 70-300  
1200 New Jersey Avenue, SE  
Washington, DC 20590

Dear Inspector General Scovel:

This letter is a written response to the questions you posed in connection with your response to inquiries directed to the Office of Inspector General from Ranking Member McCaskill and Senator Carper. These inquiries requested a review of the U.S. Department of Transportation’s (the Department’s) processes and policies for certain electronic phone applications and for responding to Congressional requests.

Throughout her tenure in the government, Secretary Chao has prioritized working with Congress on a bipartisan basis, and this includes ensuring that Congressional correspondence is responded to appropriately. This is demonstrated by the enclosed set of materials, which represents the Department’s responses to letters from members of Congress from January 20, 2017, through June 26, 2017. In total, we sent approximately 864 response letters to more than 158 different members of Congress, both in the House and the Senate. We have been responsive to members of Congress from both parties. These letters respond to a variety of Congressional correspondence, including requests received from committee chairmen, ranking members, and individual members of Congress. The Department’s Secretarial offices and Operating Administrations provided these letters, with the exception of FAA, which provided copies limited to correspondence to members of its Congressional committees. In addition to written responses, the Secretary has also engaged in many in-person and phone meetings with members of Congress from both parties.

With regard to your questions related to electronic records and smartphone applications, we recently received a similar inquiry from Chairman Chaffetz and Ranking Member Cummings. The Department’s response to that letter is enclosed, along with its attachments, which included two relevant written policies of the Department.

Except to the extent the referenced smartphone applications are addressed by the written policies just noted, the Department has not issued specific and detailed written directives about those applications in particular, but tools that automatically delete messages have not been approved or endorsed for official business use.
I hope that you find this information useful. If I can provide further information or assistance, please feel free to call me.

Sincerely,

[Signature]

Jeffrey A. Rosen

Enclosures
May 5, 2017

The Honorable Elijah E. Cummings  
Ranking Member, Committee on Oversight  
and Government Reform  
U.S. House of Representatives  
Washington, DC 20515

Dear Congressman Cummings:

I am writing in response to your March 8, 2017, letter in which you requested information related to Federal record keeping requirements and policies about the use of non-official electronic messaging accounts and social media platforms for official business. You also asked about the status of our compliance with the Managing Government Records Directive (M-12-18) issued by the Office of Management and Budget (OMB) on August 24, 2012. The Secretary asked me to respond on her behalf.

In response to your first question, a small number of senior agency officials have alternative U.S. Department of Transportation (DOT) email accounts. As with all Departmental employees, senior agency officials are assigned official e-mail user accounts that substantively follow the format of First.Last@dot.gov (or in the case of the Federal Aviation Administration (FAA), First.Last@faa.gov). In addition, the current Secretary of Transportation and FAA Administrator, as well as the previous Secretary of Transportation and previous National Highway Traffic Safety Administrator, also have used a separate DOT e-mail account for purposes of scheduling, internal communications, and other official matters.

In response to your questions two, three, and four, regarding policies in place related to non-official messaging accounts, official text message, or other messaging or communications applications and social media, and managing federal records on official electronic messaging accounts other than email, the DOT has two relevant policies that address these issues: the records management policy and the Web-based Interactive Technology Policy. Our records management policy specifically requires DOT employees and contractors “to preserve all [Federal] records, regardless of media, throughout their entire lifecycle, in accordance with applicable statutory and regulatory requirements and to promote access to information by staff, partners, and the public, as appropriate.”

In addition, DOT’s Web-based Interactive Technologies Policy provides that a Federal record disseminated via any electronic method (including electronic mail, electronic bulletin board, social media Web site, blog, or other online system) must be managed in accordance with guidance issued by the National Archives and Records Administration (NARA) and approved records retention schedules. I am enclosing copies of these two policies for your information.

In response to your fifth question, under the Freedom of Information Act, we are required to conduct a reasonable search of potentially-responsive records. In designing this search, we engage with relevant document custodians to understand which email accounts, platforms, and devices they use to conduct official business, and we construct a search accordingly. For the
The Honorable Elijah E. Cummings

senior agency officials with an alternative email accounts, we search both email accounts for potentially-responsive records.

In response to your sixth question, with respect to OMB’s Managing Government Records Directive, the latest Senior Agency Official for Records Management Report that the Department prepared for NARA is available here: https://www.archives.gov/files/records-mgmt/agency/dot-saorm-2016.pdf. Sections 2, 3, 4, and 5 of this report measure the DOT’s progress in meeting the M-12-18 directive, and the DOT has met goals 1.2, 2.1, 2.2, 2.3, 2.4, and 2.5 of the M-12-18 directive. In addition, as part of meeting this directive, the Department is following the NARA Email Management Strategy called “Capstone” and following the associated General Records Schedule 6.1. The DOT’s only outstanding goal is 1.1, which requires agencies to manage all permanent records in an electronic format by 2019. In working towards this goal, as described in DOT’s latest Senior Agency Official for Records Management Annual Report, DOT has taken actions to evaluate and implement the digitization of permanent records created in hard copy or other analog formats (e.g., microfiche, microfilm, analog video, analog audio).

I hope this information is helpful to you and the Committee. A similar letter has been sent to Chairman Chaffetz. If I can provide further information or assistance, please feel free to call me.

Sincerely yours,

Kristen Baldwin

Enclosures
May 5, 2017

The Honorable Jason Chaffetz
Chairman, Committee on Oversight
and Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am writing in response to your March 8, 2017, letter in which you requested information related to Federal record keeping requirements and policies about the use of non-official electronic messaging accounts and social media platforms for official business. You also asked about the status of our compliance with the Managing Government Records Directive (M-12-18) issued by the Office of Management and Budget (OMB) on August 24, 2012. The Secretary asked me to respond on her behalf.

In response to your first question, a small number of senior agency officials have alternative U.S. Department of Transportation (DOT) email accounts. As with all Departmental employees, senior agency officials are assigned official e-mail user accounts that substantively follow the format of First.Last@dot.gov (or in the case of the Federal Aviation Administration (FAA), First.Last@faa.gov). In addition, the current Secretary of Transportation and FAA Administrator, as well as the previous Secretary of Transportation and previous National Highway Traffic Safety Administrator, also have used a separate DOT e-mail account for purposes of scheduling, internal communications, and other official matters.

In response to your questions two, three, and four, regarding policies in place related to non-official messaging accounts, official text message, or other messaging or communications applications and social media, and managing federal records on official electronic messaging accounts other than email, the DOT has two relevant policies that address these issues: the records management policy and the Web-based Interactive Technology Policy. Our records management policy specifically requires DOT employees and contractors “to preserve all [Federal] records, regardless of media, throughout their entire lifecycle, in accordance with applicable statutory and regulatory requirements and to promote access to information by staff, partners, and the public, as appropriate.”

In addition, DOT’s Web-based Interactive Technologies Policy provides that a Federal record disseminated via any electronic method (including electronic mail, electronic bulletin board, social media Web site, blog, or other online system) must be managed in accordance with guidance issued by the National Archives and Records Administration (NARA) and approved records retention schedules. I am enclosing copies of these two policies for your information.

In response to your fifth question, under the Freedom of Information Act, we are required to conduct a reasonable search of potentially-responsive records. In designing this search, we engage with relevant document custodians to understand which email accounts, platforms, and devices they use to conduct official business, and we construct a search accordingly. For the
senior agency officials with an alternative email accounts, we search both email accounts for potentially-responsive records.

In response to your sixth question, with respect to OMB’s Managing Government Records Directive, the latest Senior Agency Official for Records Management Report that the Department prepared for NARA is available here: https://www.archives.gov/files/records-mgmt/agency/dot-saorm-2016.pdf. Sections 2, 3, 4, and 5 of this report measure the DOT’s progress in meeting the M-12-18 directive, and the DOT has met goals 1.2, 2.1, 2.2, 2.3, 2.4, and 2.5 of the M-12-18 directive. In addition, as part of meeting this directive, the Department is following the NARA Email Management Strategy called “Capstone” and following the associated General Records Schedule 6.1. The DOT’s only outstanding goal is 1.1, which requires agencies to manage all permanent records in an electronic format by 2019. In working towards this goal, as described in DOT’s latest Senior Agency Official for Records Management Annual Report, DOT has taken actions to evaluate and implement the digitization of permanent records created in hard copy or other analog formats (e.g., microfiche, microfilm, analog video, analog audio).

I hope this information is helpful to you and the Committee. A similar letter has been sent to Congressman Cummings. If I can provide further information or assistance, please feel free to call me.

Sincerely yours,

Kristen Baldwin

Enclosures
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, National Archives and Records Administration (NARA) Regulations, and the Presidential Directive on Records Management, as well as general records management at DOT.

This policy provides an overall, high-level direction to Components 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 statutes 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, while permanent records are transferred to the legal custody of the National Archives.

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.

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.

---

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
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. 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\(^\text{18}\) 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." 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 fulfill 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.\(^20\)

---

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 records 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

![Signature]

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
- 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 2012-02: Guidance on Managing Content on Shared Drives
- NARA Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18), April 2016

Table of Contents
Section 33.1 Purpose

33.1.1 The Departmental Web-based Interactive Technologies Policy establishes the U.S. Department of Transportation’s (DOT) policy for employee access, employee conduct, account management, acceptable use, approved sites, and other requirements when using Web-based interactive technologies during work hours, including employee work-related online activities, limited personal use of Web-based interactive technologies, and other Web-based interactive technologies.

33.1.2 The Departmental Web-based Interactive Technologies Policy establishes policies and responsibilities for selecting, creating, managing, and maintaining the DOT Web-based interactive technology capabilities such as social media, blogs, and video sharing.
33.1.3 DOT policy regarding the use and management of official DOT Web sites is addressed in the Chief Information Officer Policy (CIOP) Chapter 24, Departmental Web Policy – including Section 508 of the Rehabilitation Act, privacy, security, and other requirements.

Section 33.2 Background

33.2.1 This order is developed in reference to and is consistent with many existing laws and Federal policies that govern DOT information provided via the Web and interactions with the public using Web-based interactive technologies. This order also covers the use of Web-based interactive technologies where DOT employees seek to interact with one another or peers in other Federal agencies. The entire list of references can be found in Appendix D, Legal Authorities and Guidance. The order is issued under authority delegated to the Chief Information Officer (CIO) under DOT Order 1101.16A, the Organization Manual for the Office of the Secretary of Transportation, which assigns responsibility to the CIO for ensuring that DOT’s use of Information Technology (IT) complies with IT external mandates such as Section 508 of the Rehabilitation Act, Office of Management and Budget (OMB) reporting requirements, the Privacy Act, and Records Management rules.

33.2.2 The following definitions apply throughout this Directive:

- **Web-based interactive technologies** – A broad term for the wide spectrum of Web 2.0 and user-driven content technologies that allow individuals to share and edit content and collaborate online and includes such tools as blogs, wikis, social networks, video-sharing, photo-sharing, podcasts, Web feeds, social bookmarking, mashups, widgets, virtual worlds and microblogs. Often referred to as “social media.”

- **Work Related use of Web-based interactive technologies** – Use of Web-based interactive technologies that is sanctioned as part of an employee’s job function, including: (1) representing DOT online in an employee’s official capacity, when expressly authorized by the respective Operating Administration’s (OA) Office of Public Affairs (or equivalent) or Office of the Secretary of Transportation’s (OST) Office of Public Affairs, to communicate DOT’s views or position (e.g., on a site maintained or monitored by DOT); (2) using Web-based interactive technologies to further an employee’s specific job responsibilities (e.g., internal blogs or wikis for collaboration among agency project teams); or (3) for professional development purposes (e.g., using external sites to engage with other professionals in a community of practice).
• **Personal Use of Web-based interactive technologies at Work** – An employee's personal use of Web-based interactive technologies during work hours for purposes which are not part of or related to an employee's official duties whether or not it occurs on government-owned equipment (e.g. providing personal updates to social media sites).

**Section 33.3 Scope and Applicability**

33.3.1 This order applies to all DOT employees.

33.3.2 This order applies to all Web-based interactive technologies, including social media, whether they are provided via an official “.gov” Web site or by a third-party service provider.

33.3.3 This order applies to work-related use of Web-based interactive technologies and personal use of Web-based interactive technologies at work.

**Section 33.4 Policy**

33.4.1 Generally, the Department encourages the responsible use of social media by employees in support of DOT's mission, including enhancing communication and the exchange of information about DOT activities and programs with the public, Federal, State and local partners, and other interested stakeholders. When using social media, employees are bound by the same conduct and ethical rules that apply to offline conduct, including the Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR Part 2635 and the guidelines for employee conduct when using social media at work, attached herein as Appendix A.

33.4.1.1 DOT employees must follow the guidelines for employee conduct attached herein as Appendix A, as well as all policies contained in the CIOP. Failure to comply with all such directives may result in disciplinary action, up to and including removal from Federal service. Employees have no reasonable expectation of privacy for any communications executed on government-owned equipment, whether the communications are made in one's official capacity or in one's personal capacity.

33.4.1.2 Employees are expected to conduct themselves professionally in the workplace and to refrain from using Web-based interactive technologies on DOT-owned equipment for activities that are inappropriate. Behavior must comply with the “DOT Information System Responsibilities and Rules of Behavior for Users, Account Administrators, and System Operators” in accordance with Chapter 2 of the CIOP.
33.4.2 Accounts created on third-party Web-based interactive technologies for purposes of official communications must be approved by the DOT Office of Public Affairs, the DOT Office of General Counsel (OGC), and the designated Terms of Service (TOS) point of contact for each third-party tool. The DOT Office of Public Affairs must maintain a roster of official account owners with access to all official accounts for both DOT and its Operating Administrations.

33.4.2.1 The DOT Office of Public Affairs roster of official account owners must also contain the associated user names and passwords for accounts used for official communication.

33.4.2.2 The roster must be stored and properly secured. If an approved electronic content management system is utilized for storing the roster, access to the roster must be controlled using password and/or other means of encryption. If a hard copy storage method is utilized for storing the roster, access to the roster must be controlled by maintaining the roster in a locked and secure location with limited access.

33.4.3 Accounts created on third-party Web-based interactive technologies (e.g., click-through agreements) for purposes of official communication must be managed in accordance with the principles outlined in DOT Order 1351.15, Identification and Authentication Controls.

33.4.3.1 To the extent feasible, official accounts should be registered to a generic DOT e-mail address. If an account must be registered under an individual employee's DOT e-mail address, the waiver process outlined in Section 33.9 of this order must be followed.

33.4.3.2 In accordance with DOT Order 1351.15, official account owners must change the password on the third-party Web-based interactive technologies site every 90 days.

33.4.4 Only designated employees working in public engagement and/or public affairs or information technology (IT) support will be considered official account owners and have access to public-facing official Internet-based capabilities.

33.4.4.1 All official statements and/or public remarks that reflect the views of DOT or represent DOT's position in any way must be authorized as set forth in this policy, comply with applicable requirements, and be in accordance with approved procedures.

33.4.4.2 An official account owner may speak on behalf of DOT only when such commentary is based on governing law and on explicit written standards, policies and practices, and if the official account owner has received express authorization to represent DOT's views or position as set forth in this policy.

33.4.5 All Web-based interactive technologies in use on DOT equipment and networks must have a designated tool sponsor and be subject to the approval of the Chief Technology Officer (CTO), the Chief Information Security Officer (CISO), and the
OGC prior to any and all access or use. A tool sponsor is any individual making the request to the DOT Technology Control Board (TCB) that a new Web-based interactive technology be added to the certified list.

33.4.5.1 A CTO-certified list of approved and prohibited Web-based interactive technologies, and any conditions or restrictions determined, must be established. The selection of a third-party Web-based interactive technologies application for official use by the Department is subject to, at a minimum:

33.4.5.1.1 Inclusion of the third-party Web-based interactive technology on the General Services Administration’s (GSA) social media applications catalog at www.apps.gov. If a sponsor requests a technology that is not listed in the catalog, the waiver process, as outlined in Section 33.9 of this order must be followed.

33.4.5.1.2 Existing procurement laws and regulations.

33.4.5.1.3 The DOT Certification, Accreditation, and Security Assessment Policy (DOT Order 1351.6). If a Federal Risk and Authorization Management Program (FedRAMP) joint authorization is available, such information must be provided to the CTO prior to initiating Certification and Accreditation activities.

33.4.5.1.4 The Departmental Web Policy (DOT Order 1351.24), which provides for the negotiation of the Terms of Service for a third-party and the accessibility of Web-based interactive technologies.

33.4.5.2 Access to any Web-based interactive technologies that could increase the vulnerability or in any way threaten the security of the Department may be restricted or prohibited.

33.4.6 All DOT Web sites implementing Web-based interactive technology functionality must comply with the requirements of Section 508 of the Rehabilitation Act and all applicable provisions of the Departmental Web Policy, DOT Order 1351.24.

33.4.6.1 To ensure equivalent access to resources—not only for individuals with visual or hearing disabilities but for individuals who prefer not to use interactive technology to communicate with or obtain information and services from DOT—equivalent content intended to be official that is posted to a third-party platform must also be maintained on an official "gov" site, and visitors to the third-party platform must be properly directed to the official "gov" site for official content and an alternative mechanism to use for sending feedback.

33.4.6.2 If the third-party Web-based interactive technology is used to solicit feedback, an official DOT e-mail address where users can also send feedback must be provided on the official "gov" site. An official DOT telephone number and/or mailing address may also be provided.

33.4.7 DOT third-party Web-based interactive technologies must follow the privacy policies outlined in DOT Order 1351.24, including, but not limited to:
33.4.7.1 Complying with requirements to collect the minimum information necessary and to conduct an adapted Privacy Impact Assessment (PIA), as outlined in OMB Memorandum M-10-23, "Guidance for Agency Use of Third-Party Web sites and Applications." DOT will prepare and maintain a standard PIA for this purpose. Any program that will operate a third-party Web site or application in a manner that creates different privacy implications must prepare a separate, program-specific PIA, and a System of Records Notice, if required by DOT Privacy Policy, as contained in CIOP Chapters 19 and 20, or the Departmental Web Policy – CIOP Chapter 24.

33.4.7.2 Evaluating the third-party Web-based interactive technologies provider's privacy policy, monitoring the policy for changes, and periodically assessing the risks.

33.4.7.3 Posting a Privacy Notice as required by OMB Memorandum M-10-23 (see template at Appendix C) directly on the third-party site or providing a link to the Privacy Notice if posting the Notice directly on the third-party site is not feasible.

33.4.8 DOT implementations of Web-based interactive technologies must abide by intellectual property requirements.

33.4.8.1 DOT will not embed content and mediawithout verifying the right to post content, especially embedded media. In the case of copyrighted works (e.g., literature, photography, video), DOT will only post the content in the following cases:

33.4.8.1.1 DOT has the copyright in the work.

33.4.8.1.2 DOT has permission to use the work and appropriate attribution is given to the owner, creator, or artist.

33.4.8.1.3 The use of the content owner's work is permissible under statute.

33.4.8.1.4 The work falls within the fair use exception under the Copyright Right Act. (See 17 U.S.C. § 107).

33.4.9 All official DOT third-party Web-based interactive technology sites must, to the extent practical, display or direct visitors to:

33.4.9.1 An official DOT "gov" Web site for official information (to the main www.dot.gov page).

33.4.9.2 The Privacy and Intellectual Property (IP) notices, provided in Appendix C.

33.4.9.3 The Citizen Conduct Policy, Appendix B of this order, when Web-based interactive technologies allow for additional citizen conduct requirements (i.e., comment policies, take-down notices, terms of use, etc.), whether hosted on or outside a "gov" Web site address.

33.4.10 Communications from the public to DOT made through web-based interactive technologies will in no way constitute legal or official notice or comment to DOT, or any official or employee of DOT, for any purpose. Each Web-based interactive
technology site must clearly explain how any communications received from the public will be used by DOT and provide a link to information on how to submit official communications to DOT.

33.4.11 All DOT implementations of Web-based interactive technologies must comply with the Paperwork Reduction Act, the requirements of DOT Order 1351.29 (Paperwork Reduction Act (PRA) and Information Collection Request (ICR)), and the Office of Information and Regulatory Affairs (OIRA) Memorandum, "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act," as appropriate.

33.4.11.1 Specifically, the provisions of DOT Order 1351.29 apply to uses of Web-based interactive technologies in the following instances:

33.4.11.1.1 For surveys of any kind, including Web polls and satisfaction surveys.
33.4.11.1.2 Any feedback mechanism (e.g., suggestion box, brainstorming, idea generation) that requires respondents to register as a user and collects information about respondents beyond what is necessary for self-identification (i.e., only name and e-mail or mailing address are "necessary")
33.4.11.1.3 Any activity that goes beyond the scope of an in-person public meeting, including distribution of surveys or asking identical questions of 10 or more attendees.
33.4.11.1.4 Any use of a structured form to collect information, such as posting to a spreadsheet.
33.4.11.1.5 Any collection of information beyond the minimum amount of self-identification required for persons who register as users of Web-based interactive technologies for the purpose of creating accounts or profiles.
33.4.11.1.6 Any collection of information for programmatic purposes (such as form-based applications for grants).

33.4.11.2 The provisions of DOT Order 1351.29 do not apply to uses of Web-based interactive technologies in the following instances:

33.4.11.2.1 Engagements that are the functional equivalents of public meetings (i.e., not surveys), whether hosted on a "gov" Web site or by a third-party Web-based interactive technology provider.
33.4.11.2.2 General solicitations, such as notices published in the Federal Register or other Web-based interactive technologies, that request public comments on proposed regulations or any general requests for comments "regardless of the form or format thereof" (see 5 CFR 1320.3(h)(4)).
33.4.11.2.3 Unstructured solicitations that give members of the public the option of replying to some or all of the questions in the manner they prefer. A general solicitation may have a degree of specificity, such as a series of specific questions designed to elicit relevant public feedback, but may not be a survey and the responses should be unstructured.
33.4.11.2.4 Opportunities to provide general comments on discussion topics through Web-based interactive technologies (i.e., Web sites, blogs, microblogs, audio-, photo-, or video-sharing Web sites, or online message boards).

33.4.11.2.5 Opportunities to participate in a contest that involves the submission of essays, videos, software, applications, or other such materials so long as no additional information is collected for the contest beyond what is necessary to contact the entrants.

33.4.11.2.6 Subscription services, such as agency updates, alerts, notification lists, or Really Simple Syndication feeds.

33.4.11.2.7 Public interactive meeting tools—including, but not limited to, public conference calls, webinars, blogs, discussion boards, forums, message boards, chat sessions, social networks, and online communities. These tools meet the definition of an in-person public meeting.

33.4.11.2.8 When DOT collects "like items" that are not "information." These include activities where DOT Web sites may offer users the option to:

33.4.11.2.8.1 Create user accounts or profiles. When doing so, DOT third-party Web sites may collect an e-mail address, username, and password for account registration purposes and optional information such as geographic location (e.g., State or Region for statistical or other purposes).

33.4.11.2.8.2 Provide information on preferences to be used in the customization of or to influence the appearance of any given Web site.

33.4.11.2.8.3 Rate or rank (vote, flag, tag, label, or similarly assess the value of content). Dissemination of such data is subject to Information Quality Act guidelines.

33.4.11.2.8.4 Provide information necessary for the selection, payment, or delivery of an item or to identify a person ordering an item, so long as information is not collected regarding the person's qualification to participate in such a transaction.

33.4.11.3 Any personally identifiable information collected by or made available to DOT must comply with privacy requirements, as provided in Section 33.4.6, even if it does not trigger the application of the Paperwork Reduction Act and DOT Order 1351.29.

33.4.12 In accordance with DOT Order 1351.28, Records Management, information that meets the definition of a Federal record and is disseminated via any electronic method (i.e., e-mail, electronic bulletin board, social media Web site, blog, or other online system) must be documented in an official DOT recordkeeping system and retained and disposed of, or permanently preserved, in accordance with records schedules that have been approved by the National Archives and Records Administration (NARA). If information that is identified as a Federal record does not have an applicable records schedule, then the content owner must notify the business unit records management staff.
33.4.13 Advertisements and endorsements must be blocked or removed from a third-party page to the maximum extent possible. If advertisements and endorsements cannot be blocked or removed, the waiver process in Section 33.9 must be followed.

(Table of Contents)

Section 33.5 Roles and Responsibilities

33.5.1 The Office of Primary Responsibility (OPR) for this policy is the Office of the Departmental Chief Technology Officer (CTO). The CTO must:

33.5.1.1 Establish a certified list of acceptable and prohibited Web-based interactive technologies through the Technology Control Board (TCB) and make it available to Departmental employees, contractors, and guests.

33.5.1.2 Approve or prohibit the access to and/or use of any Web-based interactive technologies through the TCB.

33.5.1.3 Determine and authorize any conditions or restrictions to access and/or use any Web-based interactive technologies through the TCB.

33.5.1.4 Work with tool sponsors to develop tool-specific guidance documentation for DOT employees along with the OGC and OPA.

33.5.1.5 Participate in the waiver processes outlined in Section 33.9 for advertisements and endorsements and non-GSA approved applications for consideration in the certified list of acceptable and prohibited Web-based interactive technologies.

33.5.1.6 Manage the issuance of annual broadcast messages at the start of the fiscal year and/or employee memoranda reminding employees of the requirements in the CIOP.

33.5.1.7 Ensure that only certified Web-based interactive technologies, as determined by the DOT CTO and TCB, are linked to official Web sites.

33.5.1.8 Ensure that the DOT Linking Policy, as outlined in DOT Order 1351.24, Departmental Web Policy, is followed, including the conspicuous and clear display of the exit disclaimer.

33.5.1.9 Ensure equivalent access to resources, including posting content intended to be official that is posted to a third-party platform on an official "gov" site.

33.5.1.10 Build and maintain a page containing the privacy notice, IP notice, and citizen conduct policy for third-party Web-based interactive technologies for official purposes.
33.5.2 Secretarial Officers and Heads of OAs must:

33.5.2.1 Require all employees to comply with the Department's Web-Based Interactive Technologies Policy.

33.5.2.2 Encourage the responsible use of social media by employees in support of DOT's mission.

33.5.2.3 Assign adequate personnel and resources to satisfy the requirements of this CIOP.

33.5.3 Departmental Chief Information Officer (CIO) must:

33.5.3.1 Provide a Terms of Service Point of Contact for coordination with the Departmental Office of Public Affairs to set up official pages.

33.5.3.2 Delegate responsibility to the CTO for developing a certified list of acceptable and prohibited Web-based interactive technologies through the TCB.

33.5.3.3 Delegate the responsibility to consult account and content owners on the requirements of the Paperwork Reduction Act, as it applies to engagements with the public on behalf of DOT while using Web-based interactive technologies, to the Associate CIO for IT Policy Oversight.

33.5.3.4 Participate in all waiver processes outlined in Section 33.9.

33.5.4 Departmental Chief Information Security Officer (CISO) must:

33.5.4.1 Oversee Certification and Accreditation activities in coordination with the TCB and Cybersecurity and Privacy Council in developing and maintaining the CTO-certified list of approved and prohibited Web-based interactive technologies.

33.5.4.2 Restrict or prohibit the access and/or use of any Web-based interactive technologies tool determined to be a threat to the security of the Department.

33.5.5 DOT Privacy Officer must:

33.5.5.1 Oversee compliance with privacy policies outlined in DOT Order 1351.24.

33.5.5.2 Develop a PIA to comply with requirements as outlined in OMB Memorandum M-10-23, "Guidance for Agency Use of Third-Party Web sites and Applications" for any use of Web-based interactive technologies that deviates from the standard PIA developed by DOT OGC.

33.5.5.3 Develop and maintain, in coordination with DOT OGC, the privacy notice contained in Appendix C of this order.
33.5.6 **Departmental Office of Public Affairs (OPA)** must:

33.5.6.1 Authorize official DOT, OA, or program accounts.

33.5.6.2 Maintain a roster of employees with access to all official DOT and OA accounts.

33.5.6.3 Maintain a roster of official account owners as well as associated user names and passwords. This roster must be stored and properly secured. If an approved electronic content management system is utilized for storing the roster, access to the roster must be controlled using password and/or other means of encryption. If hard copy storage method is utilized for storing the roster, access to the roster must be controlled by maintaining the roster in a locked and secure location, with limited access.

33.5.6.4 Authorize official statements or public remarks that reflect the views of DOT or represent DOT's position in any way, including on social media sites.

33.5.6.5 Develop and make available procedures for authorizing accounts and official statements.

33.5.6.6 Consult with OGC as necessary to ensure that official commentary is based on governing law and on explicit written standards, policies and practices.

33.5.6.7 Ensure that official accounts are maintained only on certified Web-based interactive technologies, as determined by the DOT CTO and TCB.

33.5.6.8 Work with tool sponsors to develop tool-specific guidance documentation for DOT employees along with the OGC and CTO.

33.5.6.9 Develop and maintain, in coordination with DOT OGC, the citizen conduct policy contained in Appendix B of this order.

33.5.6.10 Participate in the waiver processes outlined in Section 33.9 for the inclusion of advertisements and endorsements on Web-based interactive technologies for official purposes.

33.5.7 **Office of the General Counsel (OGC)** must:

33.5.7.1 Conduct Terms of Service reviews in coordination with the TCB and Cybersecurity and Privacy Council, to help in developing and maintaining the CTO-certified list of approved and prohibited Web-based interactive technologies.

33.5.7.2 Provide advice to the TCB on the governing acquisition regulations and procedures (Federal Acquisition Regulation and/or the Transportation Acquisition Regulation, as implemented by DOT Order 4200.18B, Transportation Acquisition Manual) in developing and maintaining the CTO-certified list of approved and prohibited
Web-based interactive technologies.

33.5.7.3 Work with tool sponsors by advising them on compliance with this policy and assisting them in the development of tool-specific guidance documentation for DOT employees, along with the DOT OPA and CTO. Assist OA Chief Counsel Offices providing similar services to OA tool sponsors.

33.5.7.4 Develop and maintain, in coordination with tool sponsors and the DOT Privacy Officer, the PIA that covers standard use of Web-based interactive technologies, in compliance with requirements as outlined in OMB Memorandum M-10-23. Also, advise the DOT Privacy Officer and tool sponsors, working with OA Chief Counsel Offices as appropriate, in the development of tool-specific PIAs that deviate from the standard PIA.

33.5.7.5 Advise official account and content owners when verifying the right to post content, especially embedded media.

33.5.7.6 Develop and maintain, in coordination with the DOT Office of Human Resources, the employee conduct policy contained in Appendix A of this order.

33.5.7.7 Develop and maintain, in coordination with the DOT Privacy Officer, the privacy notice contained in Appendix C of this order.

33.5.7.8 Develop and maintain, in coordination with DOT OPA, the citizen conduct policy contained in Appendix B of this order.

33.5.7.9 Participate in the waiver processes outlined in Section 33.9 for the inclusion of advertisements and endorsements on Web-based interactive technologies for official purposes.

33.5.8 Departmental and OA Ethics Officials must:

33.5.8.1 Periodically include ethical requirements regarding use of Web-based interactive technologies in annual and/or other ethics training.

33.5.9 Departmental Disability Resource Council (DRC) must:

33.5.9.1 Conduct accessibility reviews, in coordination with the TCB, in developing and maintaining the CTO-certified list of approved and prohibited Web-based interactive technologies.

33.5.9.2 Provide guidance to all official account owners implementing DOT Web sites using Web-based interactive technology functionality to ensure compliance with the requirements of Section 508 of the Rehabilitation Act and all applicable provisions of the Departmental Web Policy, DOT Order 1351.24.

33.5.10 Departmental and OA Office of of Human Resources (HR) must:
33.5.10.1 Advise OST and OA supervisors, as needed, about taking disciplinary or other appropriate action in accordance with agency policy for violations of the policies in the CIOP, including Appendix A.

33.5.10.2 Develop and maintain, in coordination with the DOT OGC, the employee conduct policy contained in Appendix A of this order.

33.5.11 **Operating Administration Chief Information Officer (OA CIO)** must:

33.5.11.1 Coordinate with tool sponsors within their OA when sponsors submit requests to the TCB to add technologies to the approved list.

33.5.12 **Operating Administration's Web Manager** must:

33.5.12.1 Ensure that only certified Web-based interactive technologies, as determined by the DOT CTO and TCB, are linked to official Web sites.

33.5.12.2 Ensure that the DOT Linking Policy is followed, including the conspicuous and clear display of the exit disclaimer.

33.5.12.3 Ensure equivalent access to resources, including posting OA content intended to be official that is posted to a third-party platform on an official OA "gov" site.

33.5.13 **Operating Administration Office of Public Affairs (OA OPA) or equivalent** must:

33.5.13.1 Request authorization for official OA or program accounts from the DOT OPA.

33.5.13.2 Provide DOT's OPA with accurate and thorough information to include in its roster of personnel with access to all official DOT and OA accounts.

33.5.13.3 Work with DOT's OPA to authorize official statements or public remarks that reflect the views of DOT or represent DOT's position in any way, including on social media sites.

33.5.13.4 Consult with OA OCC as necessary to ensure that OA or program office official commentary is based on governing law and explicit written standards, policies and practices.

33.5.13.5 Ensure that the content posters have received express authorization by DOT's OPA to represent DOT's views or position.

33.5.13.6 Ensure that official accounts in OA are maintained only on certified Web-based interactive technologies, as determined by the DOT CTO and TCB.

33.5.14 **Operating Administration Office of Chief Counsel (OA OCC)** must:
33.5.14.1 Advise OA tool sponsors on the development of PIAs to comply with requirements as outlined in OMB Memorandum M-10-23.

33.5.14.2 Advise OA official account and content owners when verifying the right to post content, especially embedded media.

33.5.14.3 Work with tool sponsors by advising them on compliance with this policy and assisting them in the development of tool-specific guidance documentation for DOT employees, consulting with OGC as appropriate.

33.5.15 Operating Administration Records Management Officers, and/or their designees must:

33.5.15.1 Assist account and content owners if information provided on a Web-based interactive technology that is identified as a Federal record does not have an applicable records schedule.

33.5.16 Tool sponsors must:

33.5.16.1 Sponsor and develop a business case for a specific Web-based interactive technology, not contained within the certified list, to present to the TCB.

33.5.16.2 Coordinate with their OA CIO to submit the request to the TCB.

33.5.16.3 Coordinate the development of tool-specific guidance for DOT employees with the CTO, OGC and DOT OPA.

33.5.16.4 Prepare a separate PIA (and a System of Records Notice, if required) if the operation of the third-party Web site is in variance with the standard PIA developed under OMB Memorandum M-10-23.

33.5.16.5 Evaluate the third-party Web-based interactive technologies provider's privacy policy for risks, monitoring the policy for changes, and periodically reassessing the risks.

33.5.17 Official Account Owners and Content Owners must:

33.5.17.1 Ensure that all official content meets applicable requirements outlined in this policy.

33.5.17.2 Manage official accounts in accordance with the principles outlined in DOT Order 1351.15, Identification and Authentication Controls.

33.5.17.2.1 Register official accounts under a generic e-mail address. If an official account must be registered under an individual employee's DOT e-mail address, the content owner must follow the waiver process outlined in Section 33.9 of this order.

33.5.17.2.2 Change the password on the third-party Web-based interactive technology.
site every 90 days for official accounts.

33.5.17.3 Ensure any official commentary is based on governing law or explicit written standards, policies and practices, and that the employee has received express authorization by DOT's OPA to represent DOT's views or position.

33.5.17.4 Ensure visitors to the third-party platform are properly directed to an official "gov" site for official content.

33.5.17.5 Provide an official DOT e-mail address where users can also send feedback if the third-party Web-based interactive technology is used to solicit feedback.

33.5.17.6 Ensure that embedded content, whether embedded by the content owner or other participants, includes appropriate attribution to the owner, creator, or artist.

33.5.17.7 Ensure that they have the right to post content, especially embedded media, as specified by this policy.

33.5.17.8 Either display on official DOT third-party sites or direct visitors through a link to an official DOT "gov" Web site for official information and the Privacy and IP notices, provided in Appendix C, to the extent practical.

33.5.17.9 Either display on official DOT third-party sites or direct visitors through a link to the Citizen Conduct Policy in Appendix B of this order, when Web-based interactive technologies allow for additional citizen conduct requirements (i.e., comment policies, take-down notices, terms of use, etc.) whether hosted on or outside a "gov" Web site.

33.5.17.10 Clearly explain on the site how any communications received from the public will be used by DOT and provide a link to information on how to submit official communications to DOT.

33.5.17.11 Ensure the requirements of the Paperwork Reduction Act are adhered to, as specified in this policy, for all engagements with the public on behalf of DOT while using Web-based interactive technologies. Specifically:

33.5.17.11.1 Limit the use of votes and ranking information on Web-based interactive technologies to organizing, ranking, or sorting.

33.5.17.11.2 Not assume, in general, that the results of votes and ranking information on Web-based interactive technologies are statistically reliable indicators of public sentiment and, thus, not use such information as an appropriate basis for policy or planning.

33.5.17.12 Determine, in coordination with business unit records management officers, whether information on official Web-based interactive technologies that they manage, are Federal records.
33.5.17.12.1 Manage information on official Web-based interactive technologies in accordance with appropriate DOT records schedules approved by the National Archives and Records Administration (NARA) or the General Records Schedule issued by NARA.

33.5.17.13 Ensure advertisements and endorsements are removed from Web-based interactive technologies they manage. If they cannot be, owners must follow the waiver process outlined in Section 33.9.

33.5.17.13.1 Regularly monitor official pages to ensure that advertising appearing on the page does not imply DOT endorsement of a product or service and/or negatively impact the agency message being conveyed on the page.

33.5.18 Managers and Supervisors must:

33.5.18.1 Ensure that employees are aware of their responsibilities pertaining to this policy, including the Employee Conduct Guidelines contained in Appendix A.

33.5.18.2 Take prompt disciplinary or other appropriate action in accordance with agency policy and in consultation with their Human Resources Offices for violations of the policies in the CIOP, including Appendix A.

33.5.19 All DOT employees using social media must:

33.5.19.1 Exercise reasonable judgment in interpreting this policy and in making decisions about the use of Web-based interactive technologies.

33.5.19.2 Review and be familiar with all related policies that cover the use of Web-based interactive technologies, including the Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR Part 2635, and the Employee Conduct Guidelines in Appendix A.

33.5.19.3 Conduct themselves professionally in the workplace and refrain from using Web-based interactive technologies on DOT owned equipment for activities that are inappropriate, as detailed in this policy.

33.5.19.4 Not operate an official DOT or OA account without the authorization of DOT’s OPA.

33.5.19.5 Ensure that only certified Web-based interactive technologies are used, as determined by the DOT CTO and TCB.

33.5.19.6 Be mindful of the unique considerations that arise when engaging in online communications, including that such communications remain permanently available and open to being re-published in other media and are subject to libel, defamation, copyright and data protection laws.

33.5.19.7 Be mindful that they have no reasonable expectation of privacy for any communications executed on government-owned equipment, whether the
communications are made in one's official capacity or in one's personal capacity.

33.5.20 **Technology Control Board (TCB)** must:

33.5.20.1 Develop and maintain the CTO-certified list of approved and prohibited Web-based interactive technologies, in coordination with the DOT OGC, CISO and OA CIOs.

33.5.21 **Cybersecurity and Privacy Council** must:

33.5.21.1 Coordinate with the TCB on Certification and Accreditation activities in developing and maintaining the CTO-certified list of approved and prohibited Web-based interactive technologies.

33.5.21.2 Consult the CISO in restricting or prohibiting the access and/or use of any Web-based interactive technologies tool they determine to be a threat to the security of the Department.

**Section 33.6 Dates**

33.6.1 This policy is effective on the date signed, except:

33.6.1.1 The provisions pertaining to the CTO-certified list of approved and prohibited Web-based interactive technologies will be effective 6 months after the effective date.

**Section 33.7 Cancellations**

33.7.1 This policy does not cancel any other DOT orders or notices.

**Section 33.8 Compliance**

33.8.1 Failure to comply with this policy may result in disciplinary action, including removal from Federal Service.

33.8.2 Within six months of the effective date of the policy, Operating Administrations, including OST, shall develop employee training that addresses the benefits and uses of Web-based Interactive technologies. The OAs may collaborate on such training.
Section 33.9  Waivers

33.9.1  When a third-party Web-based interactive technology requires that an account be registered to an individual DOT employee's official e-mail address, a waiver must be approved and filed by the DOT Chief Information Officer. The waiver must include:

33.9.1.1  Written documentation that the Web-based interactive technology tool's Terms of Service will not permit accounts to be registered to a general e-mail address, citing the appropriate sections.

33.9.1.2  A discussion of the controls that will be put in place to ensure that, in the event of staff absence or turnover, the office sponsoring the account will be able to retain access to the account and accomplish its mission.

33.9.2  When a third-party social media tool is requested and does not have a negotiated Terms of Service in the GSA Web-based interactive technologies catalog, a waiver must be completed to initiate review activities and placed on file with the Departmental OCIO. The waiver must include:

33.9.2.1  An overview of the required Web-based interactive technology's functionality.

33.9.2.2  A functional review of the items currently registered in the GSA social Web-based interactive technologies catalog, identifying fit/gap analysis for tools already registered in the catalog.

33.9.2.3  A discussion of the unfulfilled functional requirements and the market research that has been performed for alternative tools not available from the GSA Web-based interactive technologies catalog.

33.9.2.4  A functional review of the alternatives considered, identifying a fit/gap analysis for these alternatives and the preferred solution.

33.9.2.5  A discussion of any known attempts by other DOT or Federal organizations to negotiate with the vendor of the preferred solution, and any known barriers to negotiating appropriate terms of service.

33.9.3  For any official use of Web-based interactive technology where advertisements will be present on the page, a waiver must be approved by the DOT OPA and OGC prior to use, and placed on file with the Departmental OCIO. The waiver must include:

33.9.3.1  An overview of the required Web-based interactive technology's functionality.
33.9.3.2 A description of the type and frequency of advertisements and endorsements.

(Table of Contents)

Section 33.10 Audit Procedures

33.10.1 DOT OCIO must:

33.10.1.1 Audit the register maintained by DOT OPA on an annual basis to ensure official accounts are registered to a generic DOT e-mail address. If accounts are not registered, ensure that waivers are on file.

33.10.1.2 Compare the DOT certified Web-based interactive technologies list to the GSA's apps.gov site, to ensure that all DOT approved technologies remain approved by GSA.

33.10.1.3 Review on an annual basis all official presences on third-party Web-based interactive technology sites to ensure that, to the extent feasible, the privacy notice, IP notice, and citizen conduct policy are posted or linked.

33.10.1.4 Periodically review use of Web-based interactive technologies to ensure that its use does not constitute an information collection. If so, the account owner must display the OMB control number authorizing that collection.

33.10.2 The DOT OPA must:

33.10.2.1 Audit the register they maintain of account user names and passwords on no less than an annual basis to ensure passwords have been changed according to this policy.

(Table of Contents)
Section 33.11 Approval

Nitin Pradhan
Chief Information Officer

Nov 25, 2010
Date

(Table of Contents)
APPENDIX A: Employee Conduct Policy

I. Purpose: This Appendix establishes the Department of Transportation's (DOT) policy for employee conduct when using Web-based Interactive Technologies at work, including employees' work-related online activities, as well as limited personal use of Web-based interactive technologies during work hours, whether or not using government property.

II. References:

1. Departmental Web-based Interactive Technologies Policy (Social Media and Web 2.0) (CIOP).
2. Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR Part 2635.

III. General Policy:

The Department encourages the responsible use of Web-based interactive technologies by employees in support of DOT's mission, including enhancing communication and the exchange of information about DOT activities and programs with the public, Federal, State and local partners, and other interested stakeholders. When using Web-based interactive technologies, employees are bound by the same conduct and ethical rules that apply to offline conduct, including the Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR Part 2635.

IV. Scope: This Appendix applies to all DOT employees.

V. User Responsibilities: It is the responsibility of any person subject to this Appendix who uses Web-based interactive technologies to read, understand, and follow this policy. Employees are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of Web-based interactive technologies. Employees should be mindful of the unique considerations that arise when engaging in online communications, including that such communications remain permanently available and open to being re-published in other media and are subject to libel, defamation, copyright and data protection laws. In addition, employees should be mindful that they have no reasonable expectation of privacy for any communications executed on government owned equipment, whether the communications are made in one's official capacity or in one's personal capacity.

Each Operating Administration (OA) and the Office of the Secretary (OST) are responsible for ensuring that employees are trained in the benefits and uses of Web-based interactive technologies. Any person with questions regarding the application or
meaning of this Appendix should seek clarification from the OST Office of the Chief Information Officer (CIO), OA or the Department’s Office of Human Resources, or OA or OST Counsel Offices. Failure to comply with the policies contained in this Appendix may result in disciplinary action, up to and including removal from Federal service.

VI. Definitions:

- **Web-based interactive technologies**: A broad term for the wide spectrum of Web 2.0 and user-driven content technologies that allow individuals to share and edit content and collaborate online and includes such tools as blogs, wikis, social networks, video-sharing, photo-sharing, podcasts, Web feeds, social bookmarking, mashups, widgets, virtual worlds and micro blogs. Often referred to as "social media."

- **Work Related use of Web-based interactive technologies**: Use of Web-based interactive technologies that is sanctioned as part of an employee’s job function, including: (1) representing DOT online in an employee’s official capacity, when expressly authorized by the respective OA’s Office of Public Affairs (or equivalent) or OST Office of Public Affairs, to communicate DOT’s views or position (e.g., on a site maintained or monitored by DOT); (2) using Web-based interactive technologies to further an employee’s specific job responsibilities (e.g., internal blogs or wikis for collaboration among agency project teams); or (3) for professional development purposes (e.g., using external sites to engage with other professionals in a community of practice).

- **Personal Use of Web-based interactive technologies at Work**: An employee’s personal use of Web-based interactive technologies during work hours for purposes which are not part of or related to an employee’s official duties, whether or not it occurs on government-owned equipment (e.g., providing personal updates to Web-based interactive technologies sites).

VII. Basic Principles for Employee use of Web-based Interactive Technologies

1. When representing DOT, or otherwise engaging in work-related use of Web-based interactive technologies, act with the highest level of professionalism and integrity and in accordance with the Standards of Ethical Conduct for Employees of the Executive Branch, as well as privacy and confidentiality policies, harassment and discrimination policies, conflict of interest statutes, the Hatch Act and other applicable laws and regulations.

2. Strive for transparency and openness in all communications, while protecting privacy interests, personally identifying information, and privileged or other information inappropriate for public release.

3. Use Web-based interactive technologies in a collaborative fashion to engage the public and other stakeholders in discussion and the exchange of information; limit participation to facts or authorized statements of DOT Policy (see Section VIII(1)) and ensure accuracy.
4. Identify supporting sources (include links when possible) and include a disclaimer if necessary to clarify that no endorsement is intended.
5. Identify yourself and your DOT affiliation if participating in a work-related capacity and do not make commitments or engage in activity on behalf of DOT unless expressly authorized. Use of an alias when participating in work-related Web-based interactive technologies is not encouraged. Aliases are not the same as handles or usernames, which may be permitted by some sites. Never fraudently represent your identity online.
6. Do not use discriminatory language, ethnic slurs, personal insults, obscenity or engage in any conduct that would not be acceptable in the workplace.
7. Exercise sound judgment to ensure a distinct separation between personal views and the views of DOT and include a disclaimer if necessary to clarify that your personal views are not necessarily the views of DOT.
8. Follow the Departmental Web-based Interactive Technologies Policy contained in the CIOP.

VIII. Work Related Use of Web-based Interactive Technologies: When using Web-based interactive technologies as part of an employee’s job function, the following requirements apply:

1. All official statements or public remarks that reflect the views of DOT or represent DOT’s position in any way must be expressly authorized by OA or OST Office of Public Affairs (or equivalent) and must comply with applicable requirements.
2. An employee’s participation in Web-based interactive technology activity in any other work-related capacity must be related to and consistent with the employee’s assigned duties at DOT.
3. Employees should ensure that online activities do not interfere with other aspects of their jobs.

IX. Personal Use of Web-based Interactive Technologies at Work: DOT allows for limited personal use of Web-based interactive technology sites by employees while on breaks or during lunch (e.g., minimal, incidental use to occasionally check personal e-mail or to log onto Facebook during lunch break), subject to management discretion and the following requirements:

1. An employee’s personal use and comments made at Web-based interactive technology sites may be constitutionally protected. However, any personal use of Web-based interactive technologies while at work must be in compliance with all relevant DOT policies, including, but not limited to, the Standards of Ethical Conduct for Employees of the Executive Branch, privacy and confidentiality
policies, harassment and discrimination policies, conflict of interest statutes, the Hatch Act, and other applicable laws and regulations.

2. Personal use of Web-based interactive technologies at work must be conducted in such a manner that a reader would not think that the employee is speaking for or on behalf of DOT. If an employee’s personal views on a subject of official concern is likely to be attributed as DOT’s official position, the employee should include a disclaimer that the views expressed are the employee’s own views and not necessarily those of DOT.

3. When using government-owned property and while at work, employees should be mindful of their responsibility to use official time in an honest effort to perform official duties. Excessive and/or inappropriate use of Web-based interactive technologies for personal purposes during work hours may result in disciplinary action, up to and including removal from Federal service.

X. Personal Use of Web-based Interactive Technologies outside of Work: An employee’s personal use of and comments made at Web-based interactive technology sites may be constitutionally protected. However, employees are reminded that when they are off-duty and/or not using government owned equipment, they are still bound by the Standards of Ethical Conduct for Employees of the Executive Branch. For example, employees should not misuse their DOT positions (e.g., use their government position for private gain or to imply endorsement of organizations, products or services) nor engage in partisan political fundraising. Employees should exercise sound judgment and ensure a distinct separation between their personal use of Web-based interactive technologies and their job responsibilities. If an employee’s personal views on a subject of official concern is likely to be attributed as DOT’s official position, the employee should include a disclaimer that the views expressed are the employee’s own views and not necessarily those of DOT.

XI. Employee Conduct and Use of Web-based Interactive Technologies —At a Glance

The Departmental Web-based Interactive Technologies Policy establishes DOT’s policy for employee conduct when using Web-based interactive technologies at work, whether activities are work-related or personal in nature.

DOT encourages the responsible use of Web-based interactive technologies by employees in support of DOT’s mission, including enhancing communication and exchanging information about DOT activities and programs with the public.

Your participation in Web-based interactive technologies in any other work-related capacity must be related to and consistent with your work duties. You may only speak
on behalf of DOT if you have received express authorization to represent DOT's views or position. When speaking on behalf of DOT, identify yourself and your DOT affiliation.

Make sure that all official statements or public remarks that represent DOT's position in any way are authorized by OA or OST Office of Public Affairs (or equivalent) and comply with applicable requirements.

Be careful that you do not appear to speak on behalf of DOT without authorization. If your personal views on a subject of official concern are likely to be attributed as DOT's official position, you should include a disclaimer that says: "The views expressed here are my own and not necessarily those of DOT."

When using Web-based interactive technologies, remember that you are bound by the same conduct and ethical rules that apply to offline conduct, including the Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR Part 2635. Remember that your use of Web-based interactive technologies while at work must be in compliance with all relevant DOT policies, including, but not limited to, privacy and confidentiality policies, harassment and discrimination policies, conflict of interest statutes, the Hatch Act, and other applicable laws and regulations. Be sure to read through and familiarize yourself with these policies.

You should limit your personal use of Web-based interactive technologies at work. For example, you may occasionally check personal e-mail or log onto Facebook during a break. These activities are subject to your manager's approval and several requirements detailed in this policy.

Make sure that your online activities do not interfere with other aspects of your job. When using government property and while at work, you should be mindful of your responsibility to perform official duties. Excessive and/or inappropriate personal use of Web-based interactive technologies during work hours may result in disciplinary action, up to and including removal from Federal service.

Your personal use of Web-based interactive technologies may be constitutionally protected. However, if your personal views on a subject of official concern are likely to be attributed to DOT, then you should include a disclaimer that the views expressed are your own and not necessarily those of DOT.
APPENDIX B: Citizen Conduct Policy

This policy is STANDARD LANGUAGE that must be posted, to the extent feasible, to interactive "gov" sites or third-party sites on which DOT maintains an official presence, with respect to section 33.4.9.3 of this order. This policy is outward facing, and covers the general public's conduct on our interactive sites. These policies are also commonly known as "comment policies" or "takedown notices". This policy is applicable to comments from members of the public, on interactive "gov" sites and on third-party sites on which DOT maintains an official presence.

DOT encourages the submission of comments on transportation-related issues from the public and hopes that interested individuals will submit thoughts and reactions on a regular basis. DOT also hopes that commenters will bring to our attention projects and ideas that will help us ensure that our nation has the transportation system it needs and deserves.

DOT welcomes your comments, ideas, and concerns. But, we expect conversations to follow the conventions of civil discourse. Therefore, please take the time to read this comment policy.

This page is moderated, and DOT will review all comments.

[FOR BLOGS] This is a moderated blog, and DOT will review all comments before posting them. DOT will make best efforts to review comments and post them as quickly as possible. DOT will only accept comments from bloggers 13 years or older in accordance with the Children's Online Privacy Protection Act (COPPA). If you are 12 years old or younger, you may e-mail us rather than posting a comment on this site.

DOT will not post comments and will take down comments that:

- Contain vulgar or abusive language, personal attacks of any kind, offensive terms that target specific ethnic or racial groups, or discriminatory language based on race, sex, gender, religion, national origin, age or disability
- Promote or endorse services or products
- Are off-topic- e.g., comments that do not pertain to the topic of the blog post
- Contain security sensitive information
- Contain gratuitous links to Web sites that are viewed as spam

DOT does not discriminate against any views, but reserves the right to remove comments that do not adhere to these standards. All posted comments reflect the
views of the author and do not necessarily reflect the views or position of DOT or the Federal government.

DOT will not redact or edit a comment to remove objectionable content, so please ensure that your comment contains none of the above.

Communications made through the blog will in no way constitute legal or official notice or comment to the DOT or any official or employee of DOT for any purpose. (For example, comments on a DOT Notice of Proposed Rulemaking (NPRM) must be submitted as directed in the NPRM, not through this blog.) Nor is this blog a place to file a claim, complaint, or any other form of legal or administrative notice.

When posted, the content of all comments and the commenter's identifier (valid e-mail address or an alias, if the tool provides the option to be identified by an alias) are released into the public domain, so do not submit anything you do not wish to be broadcast to the general public. To protect your own privacy and the privacy of others, please do not include personal contact information or other personally identifiable information in the body of your comment.

Remember that, as an alternative to using this public blog mechanism to communicate with DOT, you may visit the following official DOT Web site and use the e-mail address, telephone number, and/or mailing address provided there to send communications to DOT: [insert URL for an official DOT.gov site].

Please refer to DOT's Privacy Notice for information about how any personally identifiable information that is collected about you when you visit this site, or that you choose to provide when you interact with this site, may be used.
APPENDIX C: Intellectual Property and Privacy Notices

These notices are STANDARD LANGUAGE that is intended to be posted to interactive .gov sites or third-party sites on which DOT maintains an official presence with respect to section 33.4.9.2 of this order. The contents are to be adapted for use with each third-party Web site or application used by DOT. The notice must be posted on each such Web site or application and should, to the extent feasible, be conspicuous, salient, clearly labeled, written in plain language, and prominently displayed at all locations where the public might make information, including PII, available to DOT. If not feasible to post directly on the third-party Web site or application, the notice must be linked to from the site or application.

Intellectual Property Notice

Except where otherwise noted, content on this site is licensed under a Creative Commons Attribution 3.0 License. Content includes all materials posted by the Department of Transportation and its Operating Administrations. In addition, visitors to this Website agree to grant a non-exclusive, irrevocable, royalty-free license to the rest of the world for their submissions to this site under the Creative Commons Attribution 3.0 License. A copy of this license is available online at http://creativecommons.org/licenses.

Members of the public should honor intellectual property laws and post only content they have the right to post.

The contents of the following Privacy Notice comply with OMB Memorandum M-10-23, “Guidance for Agency Use of Third-Party Web sites and Applications” (see section 4.c.).

DOT Privacy Notice

[Insert name of Web site or application] is not a government Website or application; it is controlled or operated by a third-party, not by the U.S. Department of Transportation (DOT). DOT's Privacy Policy does not apply to the third-party.

If you use this Web site or application to communicate with DOT, you may be providing non-government third parties with access to personally identifiable information (PII) about you.

Any PII about you that becomes available through your use of this third-party Web site or application will not be maintained, used, or shared by DOT, except as described in the following Privacy Impact Assessment:
As an alternative to using this third-party Web site or application, you may obtain comparable information and services from DOT by visiting this official DOT Web site:

DOT's Privacy Policy applies to, and is accessible from, the above DOT Web site.
APPENDIX D: Legal Authorities and Guidance

This order is developed in reference to many existing laws and Federal policies and is issued under authority delegated to the Chief Information Officer (CIO) for issuance of Departmental Information Technology policies pursuant to 49 CFR Part 1 and DOT Order 1101.16A The following DOT policies apply:

- DOT Order 1000.14A - Official Seal and Signatures of the Department of Transportation
- DOT Order 1351.2 - Access Controls
- DOT Order 1351.6 - Certification, Accreditation, and Security Assessments
- DOT Order 1351.15 - Identification and Authentication Controls
- DOT Order 1351.20 - U.S. Department of Transportation Rules of Conduct and Consequences Policy Relative to Safeguarding Personally Identifiable Information
- DOT Order 1351.24 - Departmental Web Policy
- DOT Order 1351.28 - Records Management
- DOT Order 1351.29 - Paperwork Reduction Act (PRA) and Information Collection Request (ICR)
- DOT Order 4200.18B - Transportation Acquisition Manual

In addition, the following statutes and Executive Orders apply:

- 5 USC §301, which provides that the head of an Executive Agency or Military Department may prescribe regulations for the use of its property
- 5 CFR Part 2635 - Standards of Ethical Conduct for Employees of the Executive Branch
- Executive Order 12674 – Principles of Ethical Conduct for Government Officers and Employees.

In addition, the following Office of Management and Budget (OMB) and Office of Information and Regulatory Affairs (OIRA) Memorandum apply:

- Office of Information and Regulatory Affairs Memorandum – "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act, " (April 7, 2010)
# Previous OIG Recommendations Concerning the Management of the Preservation of Electronic Records

<table>
<thead>
<tr>
<th>Report Title and Date</th>
<th>Recommendation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit of Security and Controls Over the National Driver Register (OIG Report No. FI2008003), October 29, 2007</td>
<td>Require National Driver Register (NDR) officials to develop a standard process for states to use when requesting the manual removal of any problem driver, including the reason for the deletion.</td>
<td>Closed (October 2007)</td>
</tr>
<tr>
<td></td>
<td>Require the NDR office to verify the state’s request before removal of the problem driver’s record from the NDR database.</td>
<td>Closed (October 2007)</td>
</tr>
<tr>
<td>Process Improvements Are Needed for Identifying And Addressing Vehicle Safety Defects (OIG Report No. MH2012001), October 6, 2011</td>
<td>Establish pre-investigation processes for retaining and storing pre-investigation records, such as investigation proposals and insurance company data.</td>
<td>Closed (December 2012)</td>
</tr>
</tbody>
</table>

*Note: OIG reports are available on our website at [http://www.oig.dot.gov/](http://www.oig.dot.gov/).*