

Chapter 14-4

DOT H 1350.2

DIRMM

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF THE SECRETARY

DOT H 1350.2

July 5, 2000

CHAPTER 14

TABLE OF CONTENTS

SUBCHAPTER 14.4 - DOT INTERNET POLICY

14.101	Purpose
14.102	Scope
14.103	Goals
14.104	Definitions
14.105	Policy
14.106	Responsibilities

SUBCHAPTER 14.4 - DOT INTERNET POLICY

14.101 Purpose.

The new resources, services, and interconnectivity available via the Internet all introduce new opportunities and risks in the Department of Transportation (DOT) workplace. This policy enables DOT to take maximum advantage of the Internet's potential while mitigating associated risks.

14.102 Scope.

This policy applies to all DOT organizations that are provided Internet resources in the workplace. DOT organizations are permitted to further define sections of this policy to ensure alignment with existing internal policies and procedures.

14.103 Goal.

DOT Internet sites will be designed and technically configured, consistent with available resources to:

- (a) Satisfy DOT users and customer needs (including persons with disabilities) by enabling them to easily and promptly discover, locate, select, access, and retrieve officially approved for public dissemination information (e.g., reports, studies, catalogs, directories, facts, data, opinions, etc.);
- (b) Provide seamless, secure communications for DOT users and customers;
- (c) Streamline processes for DOT users and customers; and
- (d) Facilitate and strengthen DOT mission and program performance.

14.104 Definitions.

- (a) Cookies are messages given to a web browser by a web server. The browser stores the message in a text file called cookie.txt. The message is then sent back to the server each time the browser requests a page from the server.
- (b) DOT organizations are departmental offices, operating administrations, offices, divisions, and comparable elements of the DOT.
- (c) DOT users are individuals authorized to use the Internet as part of their assigned official duties at DOT. These include DOT employees (full or part-time), volunteers who are authorized to use Departmental resources to access the Internet, and contractor support personnel, consultants, etc.
- (d) Home Page is the top-level World Wide Web (WWW) page document that often resembles a table of contents with electronic links to other resources or files on WWW sites. It is commonly the first page displayed when connecting to a WWW server, but may also refer to the introductory page for any particular set of information on that server.
- (e) Internet Resources includes File Transfer Protocol (FTP), Gopher, Telnet, Wide Area Information Server (WAIS), and World Wide Web (WWW) services, and established electronic discussion groups available to employees, contractor support personnel, consultants, etc. using DOT computing or network resources.
- (f) Internet Service Provider is a commercial entity offering the transmission, routing, or providing of connections for digital communications, online services (site hosting, electronic mail, etc.), or network access to the Internet.
- (g) Posting is the act of placing information on a server connected to a network. Posted information may include mailings, handouts, brochures, faxes, and press releases, and responses to inquiries, discussion of policy, and any other dissemination of information in any format.
- (h) Server is a computer system that provides a service to another known as a client.
- (i) Warnings/Disclaimers are statements that warn a user of the limitations and conditions on use of DOT resources on the Internet and similar media, including disclaimers of responsibility for the use of DOT information, notice of use audits and computer system monitoring, and Privacy Act/sensitive information restrictions.
- (j) Web Managers/Webmasters are those persons who manage the information technology and/or content aspects of websites, such as user accounts, space allocation, page or site design, or program interfaces.

14.105 Policy.

DOT Internet resources will be used -- within prescribed mandates, laws, and restrictions -- to improve information dissemination and to conduct Departmental business transactions with the public.

- (a) Increased Reliance on Website Dissemination. DOT Internet sites will be developed, within budgetary constraints, to make government information more easily accessible and useful to DOT organizations and our customers. The following are examples of conditions in which dissemination via the Internet is appropriate and encouraged:
 - (1) Provide public access to large, highly-detailed volumes of information;
 - (2) DOT knows a substantial portion of its information-seeking customers have ready access to the Internet;
 - (3) DOT information gathering or dissemination is done frequently and/or to a significant, varied customer base;
 - (4) Becoming reliant on Internet as the sole means of disseminating information will not impose substantial acquisition or training costs on users, especially state and local governments and small business entities; and
 - (5) DOT use of the Internet supports Presidential, legislative, regulatory, or agency initiatives (e.g., Electronic Freedom of Information Act, Electronic Commerce, Government Information Locator Service, etc.).
- (b) Use of DOT Internet Resources. DOT Internet resources shall be available only for authorized activities, as detailed in this section.
 - (1) Authorized Use. DOT Internet resources may be used:
 - (a) For valid work requirements (e.g., exchange of information that supports the DOT mission, goals, and objectives; job-related professional development for DOT management and staff; access scientific, technical, and other information which has relevance to DOT; and communications with peers in other Government agencies, academia, and industry); and
 - (b) For limited incidental personal use (e.g., brief communications, brief Internet searches, job-searching in response to Federal Government downsizing), provided such use does not:
 - i. Directly or indirectly interfere with DOT

computer or networking services;

- ii. Burden DOT with additional incremental cost;
- iii. Interfere with a DOT users' employment or other obligations to the government; and
- iv. Reflect negatively on DOT or its employees.

(2) Unauthorized Use. Improper use of DOT Internet resources includes:

- (a) Use for any purpose that violates the law;
- (b) Deliberate concealment or misrepresentation of identity or affiliation in electronic mail (e-mail) messages;
- (c) Unauthorized access to, or alteration of source or destination addresses of e-mail;
- (d) Actions that interfere with the supervisory or accounting functions of computer resources, including attempts to obtain system privileges unless authorized by system owners;
- (e) Propagation of chain letters, broadcasting inappropriate messages (e.g., non-business matters) to lists or individuals, and comparable resource-intensive unofficial activity;
- (f) Use of DOT Internet resources for any commercial purpose (unrelated to official activity), for financial gain (including gambling), or in support of outside individuals or entities;
- (g) Transmitting, collecting, or storing defamatory, discriminatory, obscene (including sexually explicit materials), or harassing messages or material;
- (h) Posting to external newsgroups, bulletin boards, or other public forums, unless it is a business-related requirement and appropriate office approvals have been obtained;
- (i) Engaging in matters directed towards any unauthorized fundraising, lobbying, or partisan political activities;
- (j) Causing a denial of Internet service to any legitimate DOT user;
- (k) Collecting information for use beyond the immediate transaction (except as specifically noted in the stated website privacy policy statement); and

- (1) Selling or providing information collected on Departmental websites for commercial use.
- (c) Conduct on the Internet by DOT Users. Standards of ethical conduct and appropriate behavior apply to the use of DOT computer networks, including the Internet. All DOT users shall conduct activities on the Internet with the same integrity as in face-to-face business transactions. Any illegal, harassing, discriminatory or obscene use, in violation of other DOT policies can be the basis for disciplinary action, up to and including termination or judicial sanction.
 - (d) Internet Security. DOT users, managers, and administrators using DOT Internet resources shall receive initial and periodic security awareness training appropriate for their use on the Internet. DOT Internet sites shall provide for security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information contained therein.
 - (e) Internet Privacy. DOT will ensure people's right to privacy is protected when visiting our public websites. To this end, the following phased approach has been adopted:
 - (1) DOT organizations should conduct assessments of its websites to determine what information is being collected, how the information is used, with whom the information may be shared, and the security procedures in place to protect the loss, misuse, or alteration. Based on your review, strong internal policies and procedures should be developed and instituted to protect personal information. In addition, a privacy policy statement conforming to OMB privacy policy guidance should be displayed on all DOT domain level homepages (e.g., fhwa.dot.gov) and on all DOT webpages that are major entry points to websites where personal information is collected from the public. The privacy statement included on all DOT webpages that are major entry points to web sites where substantial personal information is collected from the public should address the items indicated in Appendix C.
 - (2) As of January 1, 2000, implementation of DOT privacy policy shall include:
 - (a) Notifying visitors to DOT websites (using language the same or similar to that shown in Appendix C) when leaving DOT websites; and
 - (b) Prior to establishment of any new hotlink from a DOT website to a non-DOT website, sending non-DOT organizations (using language the same or similar to that shown in Appendix C) a notification advocating posting a statement of their website privacy policies and practices.

- (f) Management and Administration of DOT Internet Activities. The DOT Internet connection is an organizational resource. Use of DOT Internet resources shall be managed in a manner that is consistent with good customer service principles, employs sound business practices, and effectively represents the best interests of the Department.
- (1) Monitoring of Internet Usage. DOT users should be aware that they have no expectation of privacy while using any Government-provided access to the Internet. DOT management reserves the right to periodically monitor employees' use of any DOT computer system or network, including the Internet. The DOT Internet connection is an organizational resource. Activities may be subject to monitoring, recording, and periodic audits to ensure they are functioning properly and to protect against unauthorized use. In addition, authorized personnel may access any user's computer accounts or communications. Authorized personnel may disclose information obtained through such auditing to appropriate third parties, including law enforcement authorities or Freedom of Information Act requesters. Use of DOT Internet resources is expressly acknowledged by each user to be subject to such monitoring, recording and auditing.
 - (2) Usage Statistics. As a management function, evaluation of site usage data (log files) is a valuable way to evaluate the effectiveness of websites. However, collection of data from publicly accessible sites for undisclosed purposes is inappropriate. There are commercially available software packages that will summarize log file data into usable statistics for management purposes, such as the most/least requested documents, type of browser software used to access the website, etc. Use of this type of software is appropriate, as long as there is full disclosure as specified in the privacy and security notices (see Appendices C and D) and as long as there is compliance with records management storage and disposal requirements.
 - (3) User-Identifying Collection Methods for Public Websites. In accordance with the privacy and security notices (Appendices C and D), it is prohibited to use methods which collect user-identifying information such as extensive lists of previously visited sites, e-mail addresses, or other information to identify or build profiles on individual visitors to publicly accessible websites. "Cookies" should not be used by DOT web sites, or by contractors when operating web sites on behalf of DOT, unless, in addition to clear and conspicuous notice, the following conditions are met: a compelling need to gather the data on the site; appropriate and publicly disclosed privacy safeguards for handling of information derived from "cookies"; and

Secretarial approval should be requested through the Office of the CIO who will expedite the approval process. In addition, all DOT web sites shall comply with the standards set forth in the Children's Online Privacy Protection Act of 1998 with respect to the collection of personal information online at web sites directed to children.

- (4) Feedback Mechanisms. Because of the strategic importance of the Internet in executing DOT's mission and programs, DOT organizations are strongly encouraged to establish information-sharing forums to solicit input from DOT users and customers about the DOT Internet site effectiveness in terms of message conveyance, information content quality, responsiveness, ease of use, etc.
- (5) Compliance with Applicable Laws, Regulations, etc. A number of requirements contained in laws, regulations, Executive Orders, and departmental directives guide DOT Internet use (see Appendix A for some of the key ones). DOT organizations shall ensure that DOT users comply with applicable federal and departmental requirements.
- (6) Decisional Authority. Every DOT Internet site shall designate one or more person(s) as accountable for making day-to-day decisions about Internet site development and maintenance, content, consistency/linkage with other DOT Internet sites, infrastructure investments, technical operations, etc.

14.106 Responsibilities.

- (a) DOT Chief Information Officer is responsible for:
 - (1) Issuing policy and procedural guidance with respect to establishing, operating, and maintaining Web sites.
 - (2) Advising other DOT organizations on the proper and/or effective use of the Internet consistent with established IT architectures and capital investments.
 - (3) Approving top-level domain registrations.
- (b) DOT Operating Administrators and Departmental Officers are responsible for implementing this policy within their respective organizations, including delegating authority and holding delegates (e.g., network administrators, systems security officers, content managers, web designers, webmasters, etc.) accountable for their actions. Functions for which DOT Operating Administrators and Departmental Officers are responsible include:
 - (1) Disseminating departmental policies and procedures to employees on the proper use of DOT computing facilities to access the Internet.

- (2) Working with DOT officials (e.g., Freedom of Information Officers, public affairs staffs, records management officers, information architects, Privacy Act officers, Information collection officers, etc.) to ensure content placed on DOT Internet sites adheres to regulatory and departmental policies, procedures, or practices.
- (3) Providing Internet access and associated computer security training to employees who need to conduct official business via the Internet.
- (4) Efficiently managing Internet facilities to ensure only authorized equipment and software necessary to perform official government business are procured and maintained.
- (5) Assuming responsibility for making final determinations as to the appropriateness of employee use of the Internet, when questions arise, including the acceptability of Internet sites visited and the determination of personal time versus official work hours.
- (6) Establishing a process for the identification of information appropriate for posting to websites and ensuring it is consistently applied.
- (7) Establishing WWW sites which:
 - (a) Have a clearly defined purpose(s);
 - (b) Employ high standards for quality and utility;
 - (c) Provide for adequate management oversight of the website;
 - (d) Offer feedback mechanisms;
 - (e) Ensure operational integrity of the computer and network supporting the Internet site;
 - (f) Include information that is accurate, up-to-date, and clearly reflects the stated purpose of the Internet site;
 - (g) Include notices (i.e., security and privacy, disclaimer(s)), where appropriate on each DOT Internet site and transmit standard notifications when leaving DOT websites and when establishing new non-federal government links on DOT webpages, consistent with language in Appendices B, C, and D;
 - (h) Are designed to address: accessibility issues for persons with disabilities

(<http://www.w3.org/WAI/>); low-speed modem interfaces or text-only browsers; conformity to DOT organization style and content guidelines; and standardized formats (such as GIF, JPEG, and MPEG); and

- (i) Prohibit commercial sponsorships, advertisements and endorsements on publicly accessible websites under their purview.
- (8) Prevent excessive proliferation of DOT web servers and Internet sites for distribution of information.
 - (9) Complying with established DOT standards for Internet addressing.
 - (10) Obtaining approval from the Departmental Chief Information Officer (CIO) prior to entering into any agreements with commercial Internet Service Providers.
 - (11) Establishing appropriate security and operational procedures and audits to ensure continued system operation and data integrity, including:
 - (a) Providing user authentication at DOT firewall(s) for users wishing to establish a real-time connection with DOT internal computers via the Internet (see DOT H 1350.2, Chapter 11, Information Systems Security Policy);
 - (b) Ensuring that DOT Internet Servers and any data to be accessed by the general public are controlled as separate areas by the DOT firewall(s) or located external to DOT firewalls;
 - (c) Disabling, unless a specific Internet Service is needed or required, Internet traffic to prevent unauthorized access to DOT computer and networking systems; and
 - (d) Ensuring that information systems security reviews are completed before any Internet site becomes operational.
 - (12) Obtaining, with assistance of the CIO, prior approval from the Office of Management and Budget for all information collections subject to the Paperwork Reduction Act of 1995 before hosting the collection on DOT Internet sites.
 - (13) Ensuring that records management responsibilities are adequately discharged with respect to Internet sites.
 - (14) Ensuring compliance with this policy for those functions, missions, agencies, and activities under their purview.

- (c) DOT Users are responsible for:
- (1) Adhering to federal and departmental policies and procedures with Internet implications.
 - (2) Familiarizing themselves with special requirements for accessing, protecting, and utilizing data, including Privacy Act materials, records management, copyrighted materials, and procurement sensitive data, etc.
 - (3) Refraining from any practices which might jeopardize the security of the Department's computer systems and data files, including but not limited, to computer virus attacks.
 - (4) Understanding that there are no privacy expectations when using DOT computing facilities to access the Internet and that communications are not automatically protected from third-party viewing.
 - (5) Supporting strict adherence to software vendors' license agreements.
 - (6) Learning about Internet etiquette, customs, and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.
 - (7) Conducting themselves in a way that reflects positively on DOT when using the Internet.

APPENDIX A

KEY GOVERNMENT GUIDANCE WITH POTENTIAL INTERNET IMPACT

1. Americans with Disabilities Act of 1990 (42 USC 12101 note).
2. Children's Online Privacy Protection Act of 1998 (13 USC 1301)
3. Computer Fraud and Abuse Act of 1986 (18 USC 1001 note, 1030).
4. Computer Security Act of 1987 (15 USC 271 note, 272, 278g-3, 278g-4, 278h; 40 USC 759, 759 note).
5. Electronic Communications Privacy Act of 1986 (18 USC 1367, 2232, 2510, 2510 notes, 2511 to 2521, 2701, 2701 note, 2702 to 2711, 3117, 3121, 3121 note, 3122 to 3127).
6. Federal Advisory Committee Act (5 USC Appendix 1).
7. Federal Records Act (44 USC Chapters 29, 31, 33, and 35).

8. Freedom of Information Act (5 USC 552, 552 notes).
9. Paperwork Reduction Act of 1995 (5 USC Chapter 35).
10. Privacy Act of 1974 (5 USC 552a, 552a note).
11. Section 508 of the Rehabilitation Act of 1973 (as amended by the Workforce Investment Act of 1998 (29 U.S.C. 794d)).
12. OMB Circular A-130, "Management of Federal Information Resources," 61 FR 6428 (February 20, 1996).
13. Executive Orders 12674 and 12731 "Principles of Ethical Conduct of Government Officers and Employees," 5 CFR Part 2635 "Standards of Ethical Conduct for Employees of the Executive Branch," 5 CFR Chapter L and 49 CFR Part 99 "Supplemental Standards of Ethical Conduct for Employees of the Department of Transportation."
14. Executive Order 13103, "Computer Software Piracy."
15. DOT H 1350.2, Chapter 14-3, "Electronic Mail Policy."
16. DOT H 1350.250, "DOT Information Systems Security (ISS) Guide" & DOT H 1350.251, "DOT Network Security Guide."

APPENDIX B

UNITED STATES DEPARTMENT OF TRANSPORTATION
DISCLAIMER AND LIABILITY NOTICE

This website and the information it contains are provided as a public service by the U.S. Department of Transportation (DOT). This system is monitored to ensure proper operation, to verify the functioning of applicable security features, and for comparable purposes. Anyone using this system expressly consents to such monitoring. Unauthorized attempts to modify any information stored on this system, to defeat or circumvent security features, or to utilize this system for other than its intended purposes are prohibited and may result in criminal prosecution.

RESTRICTION OF LIABILITY

The DOT makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the contents of this website and expressly disclaims liability for errors and omissions in the contents of this website. No warranty of any kind, implied, expressed or statutory, including but not limited to the warranties of non-infringement of third party rights, title, merchantability, fitness for a particular purpose and freedom from computer virus, is given with respect to the contents of this website or its hyperlinks to other Internet resources. Reference in this website to any specific commercial products, processes, or services, or the use of any trade, firm or corporation name is for the information and convenience of the

public, and does not constitute endorsement, recommendation, or favoring by DOT.

OWNERSHIP

Information presented on this website is considered public information and may be distributed or copied. DOT shall have the unlimited right to use for any purpose, free of any charge, all information submitted to DOT via this site except those submissions made under separate legal contract. DOT shall be free to use, for any purpose, any ideas, concepts, or techniques contained in information provided to DOT through this site.

LINKS TO OTHER SITES

The Department of Transportation's websites have many links to other organizations, such as state/local governments, educational institutions, and non-profit associations. While we offer these electronic linkages for your convenience in accessing transportation-related information, please be aware that when you exit Department of Transportation websites, the privacy policy stated on our websites may NOT be the same as that on other websites.

Appendix C

STANDARD DOT PRIVACY NOTICE

We collect no personal information about you when you visit our website unless you choose to provide this information to us. However, we collect and store certain information automatically.

Here is how we handle information about your visit to our website.

What We Collect and Store Automatically

If you do nothing during your visit but browse through the website, read pages, or download information, we will gather and store certain information about your visit automatically. This information does not identify you personally. We automatically collect and store only the following information about your visit:

1. The Internet domain (for example, "xcompany.com" if you use a private Internet access account, or "yourschool.edu" if you connect from a university's domain) and IP address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the Web) from which you access our website;
2. The type of browser and operating system used to access our site;
3. The date and time you access our site;

4. The pages you visit; and
5. If you linked to our website from another website, the address of that website.

We use the information we collect to count the number and type of visitors to the different pages on our site, and to help us make our site more useful to visitors like you.

If You Send Us E-mail

You may choose to provide us with personal information, as in e-mail with a comment or question. We use the information to improve our service to you or to respond to your request. Sometimes we forward your e-mail to other government employees who may be better able to help you. Except for authorized law enforcement investigations, we do not share our e-mail with any other outside organizations.

Links to Other Sites

Our website has many links to our partners, especially other federal agencies. In a few cases we link to private organizations. When you link to another site, you are no longer on our site and are subject to the privacy policy of the new site.

STANDARD NOTIFICATION WHEN LEAVING DOT WEBSITE

Our websites have many links to other organizations, such as state/local governments, educational institutions, and non-profit associations. While we offer these electronic linkages for your convenience in accessing transportation-related information, please be aware that when you exit our websites, the privacy policy stated on our websites may NOT be the same as that on other websites.

STANDARD NOTIFICATION TO BE SENT BEFORE ADDING NEW HOTLINK TO DOT WEBPAGE

The Department of Transportation advocates providing useful transportation information to the general public. For this reason, we have decided to provide a hotlink to your website from ours. However, we believe it is important to address the growing public concern about protecting people's privacy on the Internet, and therefore strongly encourage you to post a statement on your website clearly describing your privacy policies and practices. Examples of privacy policies which you may want to adopt or tailor as appropriate for your website can be found at <http://cio.ost.dot.gov>. Should we receive complaints from our constituents about privacy concerns with respect to your website, we will re-consider continuing to provide linkage to your website from ours.

fNote: specific DOT organization name may be substituted where "Department of Transportation" appears in the preceding standard

notificationa

PRIVACY STATEMENT FOR WEBSITE THAT COLLECT PERSONAL
INFORMATION

The privacy statement included on all DOT webpages that are major entry points to web sites where substantial personal information is collected from the public should address the items indicated below:

- . Collection and Use of Information - Disclose the means by which you collect information both with your users' explicit knowledge (registration forms, order forms, etc.) and without their explicit knowledge (logged files, cookies)
- . Who - Who is Collecting the Information
- . Use and Sharing - Use of the Information Collected and if/how it is being shared
- . Security - Inform users what types of security procedures you have in place to protect the loss, misuse, or alteration of the information collected
- . Data Quality and Access - Provide users with a mechanism to correct and update their pertinent personally identifiable information.

Appendix D

SECURITY NOTICE

The following notice and consent banner, may be used on all DOT websites with security and access controls.

** WARNING ** WARNING ** WARNING **

This is a United States Department of Transportation (DOT) computer system. DOT systems, including all related equipment, networks, and network devices (specifically including Internet access) are provided for the processing of official U.S. Government information only. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes to consent to these terms.

** WARNING ** WARNING ** WARNING **