

Department of Commerce Internet Use Policy

1. Purpose.

This document states the Department's policy and provides guidance for managing the use of the Internet by operating units and other organizational components, and by employees within Commerce.

The goal is to ensure economical, effective and efficient management of Internet usage and encourage collaborative efforts among the Commerce components to achieve this end.

2. Contents.

<u>Topic</u>	<u>Paragraph</u>
Information and Assistance	3
Definitions	4
Background	5
Scope	6
Policy	7
Responsibilities	8

3. Information and Assistance. Guidance on this policy may be obtained from:

Office of Systems & Telecommunications Management (OSTM)
HCH Building, Room 6086
202-482-0120

4. Definitions

Internet - A global web connecting more than a million computers. Currently, the Internet has more than 30 million users worldwide, and that number is growing rapidly. More than 100 countries are linked into exchanges of data, news and opinions. Unlike online services, which are centrally controlled, the Internet is decentralized by design. Each Internet computer, called a host, is independent. Its operators can choose which Internet services to provide to its local users and which local services to make available to the global Internet community. Remarkably, this anarchy by design works exceedingly well.

World Wide Web (WWW or "Web") - A system of Internet servers that supports specially formatted documents. The documents are formatted in a language called HTML (HyperText Markup Language) that supports links to other documents, as well as graphics, audio, and video files. This means you can jump from one document to another simply by clicking on hot spots. Not all Internet servers are part of the World Wide Web.

There are several applications called Web browsers that make

it easy to access the World Wide Web; three of the most popular being Mosaic, Netscape Navigator and Microsoft's Internet Explorer.

Home Page - The main page of a Web site. Typically, the home page serves as an index or table of contents to other documents stored at the site.

Site - A site (location) on the World Wide Web. Each Web site contains a home page, which is the first document users see when they enter the site. The site might also contain additional documents and files. Each site is owned and managed by an individual, company or organization.

Firewall - A system or combination of systems that enforce a boundary between two or more networks. A network firewall, or packet filter, examines traffic at the network protocol level. An application-level firewall also readdresses outgoing traffic so it appears to have originated from the firewall rather than the internal host.

5. Background.

The Internet, a public telecommunications service, was established as a cooperative effort providing worldwide networking services among educational institutions, government agencies and various commercial and non-profit organizations. High speed networking technologies and developments have made the Internet a desirable source for expanding research interest and information dissemination and communications. The Internet has expanded to include government information, educational information systems, archives and business resources. The Internet also includes functions such as those for electronic mail (e-mail), remote computer networks, file transfers, World Wide Web (WWW) and wide area information servers.

The Department's access and use of Internet have grown exponentially. On-line services, such as the WWW, have greatly increased user access to a wider and more diverse user community of information resources. This dramatic increase in communication capabilities makes it necessary to establish policies regarding the proper and efficient use of Internet.

6. Scope.

The Internet is considered to be a fundamental communications tool that may be used to support the Department's missions and information dissemination requirements. These policies and guidelines apply to the management of Internet services within all organizational units of the Department and may be supplemented by additional guidelines developed by departmental operating units, including the use of Government provided telecommunications resources in employees' private residences. To the extent that existing Department-wide policies and directives relating to e-mail and the Internet are inconsistent

with this policy, this policy shall supersede the previous policies or directives. The Departmental Public Affairs office and other operating unit offices may also issue policy regarding the content and management of Internet data and information.

7. Policy.

It is the policy of the Department to allow and encourage the use of Internet services to support the accomplishment of the various missions of the Department. Use of the Internet requires responsible judgement, supervisory discretion and compliance with applicable laws and regulations. Users must be aware of information technology security and other privacy concerns. Users must also be aware of and follow management directives for Internet usage.

Internet services provided by the Department, like other Government equipment and resources, are to be used only for authorized purposes. The Department recognizes that it is in the interest of the Government that Department personnel become proficient and maintain proficiency in using the Internet. To this end, the restrictions outlined below regarding Internet use during official working hours and non-working hours should be followed by Department employees using Internet services provided by the Department.

The following specific statements reflect official guidance on Departmental use of the Internet:

- a. Internet services provided by the Department during official working hours are to be used for authorized purposes only. This may include using Internet services to train personnel on using the Internet, provided prior approval is obtained from an employee's supervisor.
- b. Internet service represents a corporate resource that must be managed in an efficient and cost effective manner. Departmental operating units should establish guidelines for accountability and responsibility for use of the Internet and e-mail by their respective employees.
- c. Internet access should be achieved using standard and commonly available tools, unless a specific requirement calls for a unique approach. The Department's Office of Systems and Telecommunications Management should be informed in advance of requirements for unique solutions or approaches.
- d. Operating units should ensure that their presence on the Internet fulfills mission requirements in a professional manner. Operating units should also ensure that information that they make available via the Internet is accurate, relevant, up-to-date, and is professionally

presented.

- e. Operating units and Departmental offices may use the Internet to exchange information with the public and internally as an information technology tool. It is to be considered as one of a number of tools and an alternative commercial communication network that is available to DOC.
- f. Information technology security requirements shall be a primary consideration in the decision process leading to the use of the Internet. Operating Units must take adequate precautions when processing data or storing data on computers connected to the Internet and when transmitting data on or through the Internet. Chapter 10 of the Department's Information Technology Management Handbook defines certification and accreditation requirements for all sensitive and classified general purpose and application systems. These certification and accreditation requirements apply to use of the Internet for processing or transmitting sensitive or classified data. For classified data, the Director of the Office of Security is the Department's Principal Accrediting Authority and the Director for Budget, Management and Information and Deputy Chief Information Officer is the Designated Approving Authority.

Chapter 10 of the IT Management Handbook also addresses malicious software concerns. Given the extreme vulnerability to viruses and other malicious software occasioned by use of the Internet, operating units must ensure that processes and procedures to minimize risk from malicious programs are in place. Operating units may require that virus checking software be used in conjunction with Internet use.

- g. Unless prohibited by the specific policies of the employee's bureau/operating unit, the use of Internet services and e-mail provided by the Department during non-working hours is not limited to official purposes only. This policy will assist employees in becoming proficient in using the Internet and will enhance their professional development at de minimis expense to the Government. However, employees may not use government printers or supplies in conjunction with personal Internet and e-mail activities. Activities for which Department Internet and e-mail services may not be used, during working or non-working hours, include the following:
 - (1) the pursuit of private commercial business activities or profit-making ventures (i.e., employees may not operate a business with the use of the Department's computers and Internet resources);
 - (2) matters directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group;

- (3) prohibited direct or indirect lobbying;
- (4) use of Internet sites that result in an additional charge to the Government;
- (5) engaging in prohibited discriminatory conduct;
- (6) the obtaining or viewing of sexually explicit material;
- (7) any activity that would bring discredit on the Department; or
- (8) any violation of statute or regulation.

Of course, the Department expects employees to conduct themselves professionally while using Department resources, and employees must refrain from using Department resources for activities that are disruptive to the work place or in violation of public trust.

Like all other Government computer use, use of Government equipment for personal use of the Internet may be monitored and recorded. Anyone using Government equipment consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity or employee misconduct, system personnel may provide the evidence of such monitoring to Department and law enforcement officials. Individuals are not guaranteed privacy while using government computers and should, therefore, not expect it. To the extent that employees wish that their private activities remain private, they should avoid using the Department's Internet or e-mail for such activities.

- h. Unless prohibited by the specific policies of the employee's bureau/operating unit, limited personal use of e-mail during duty hours is permissible, as such use will help promote proficiency in electronic communications, including use of the Internet, and provides an alternative method for authorized personal communications, which will promote Government efficiency.

At no time may Government e-mail addresses be used in a manner which will give the impression that an otherwise personal communication is authorized by the Department.

Personal use of e-mail cannot interfere with the official business of the employee or organization, such as spending an inappropriate amount of time during duty hours (e.g., sending more than four brief messages per day), filling up a mailbox with personal messages so as to prevent official messages from being delivered, or disseminating chain letters.

8. Responsibilities.

- a. Operating units and Departmental offices must ensure that employees are aware of these policies and guidelines. Ultimately, it is the responsibility of the management

official or supervisor who provides the equipment and/or Internet access to carry out this Internet Use Policy. Accordingly, these organizations should:

- (1) Designate a point of contact within each bureau for discussion and coordination of Internet usage and notify OSTM of the representative appointed.
- (2) Assure that use of the Internet by the operating unit and its members is consistent with these policies and guidelines and applicable laws, including the Privacy Act and the Paperwork Reduction Act.
- (3) Coordinate and oversee their organization's Internet activities and network data management.
- (4) Establish their own procedures as necessary to promote Department-wide interoperability and cooperation.
- (5) Provide the necessary technical safeguards for appropriate availability, integrity and confidentiality of operating unit systems and procedures.
- (6) Adhere to established Departmental electronic mail and network address management policies where applicable.
- (7) Participate in the development of Internet information content, usage policy and operating standards with OSTM when requested.
- (8) Assess and validate organizational needs for Internet access using their own established business practices and mission program requirements.
- (9) Determine appropriate management controls and technical safeguards to be used for Internet usage, establishing supplemental Internet use procedures and user guidelines as necessary. Because the connection of existing user networks to the Internet presents security risks, the use of firewall technology between local networks and the Internet should be considered.
- (10) Periodically assess the effectiveness of their established management controls for Internet access within their organization.
- (11) Provide access mechanisms in accordance with Department policy for Internet connectivity for employees who have an authorized purpose for Internet access from home or on authorized travel.

b. Operating unit and Departmental office users of Commerce

network resources must:

- (1) Coordinate Internet access and Internet services with the appropriate telecommunications, network management, and program management officials. Coordination will include, at a minimum:
 - * Method and type of communications access.
 - * Internet host and domain names.
 - * TCP/IP addresses.
 - * Domain Name Services.
 - * Internet applications e.g., file transfer protocol (ftp), WWW, and others.
 - * Network security and data integrity.
- (2) Ensure that basic principles of accountability and responsibility apply to electronic data dissemination and the use of the World Wide Web.

- c. DOC organizational units are encouraged to develop WWW sites that display creativity and mission focus. However, operating units should ensure that all Web sites within their organization:
- (1) Are subject to appropriate management controls.
 - (2) Remain official information sources over which the Department retains complete editorial control.
 - (3) Are not "personal" home pages or contain personal information unrelated to official business (e.g., in no circumstance should Department-supported Web sites include items such as vacation or family photographs, links to an employee's personal interest information, or links to partisan political organizations).
 - (4) Clearly display the DOC seal or text indicating DOC affiliation.
 - (5) Clearly display the operating unit's seal, emblem, logo or text indicating the title of the organization.
 - (6) Contain a uniform resource locator (URL) reference to the main Department of Commerce Home Page. (<http://www.doc.gov>).
 - (7) Contain appropriate contact information (such as name, phone number, and e-mail address) for technical and content questions.
 - (8) Include only links to Government sites and to non-government sites that are directly related to the Department's mission or necessary to carry out the Department's business. If links to non-government sites are referenced, operating units should provide a clearly visible statement specifying that the Department of Commerce does not endorse any particular product, company, information provider, or the content of the referenced sites. However, if the link is included as part of legitimate and approved export promotion activities, the statement need not disclaim the companies or products at issue.
 - (9) Are not used for direct or indirect lobbying, including links to sites which engage in or advocate indirect lobbying.
 - (10) Adhere to any future directives on DOC Web management.
- d. Use of Trademarks & Service Marks: When using any trademarks or service marks, it is recommended that the ™ (TM) or ® (R) symbols be used, as appropriate. By definition, trademarks are used to identify tangible goods, while service marks are used to identify services (including the provision of online databases).

The ™ (TM) symbol is used on marks that are considered to be trademarks by the Department but have not yet been registered. The ® (R) symbol is used only where the mark is actually registered with the U.S. Patent & Trademark

