

	Department of Commerce OFFICE OF THE CHIEF INFORMATION OFFICER	<input type="text"/>	Search	
				
	Home	About OCIO	Contact Us	Site Map
You Are Here: OCIO > Policy and Programs > IT Policy, Guidance & Legislation > Social Media - Web 2.0 Policy 				
<hr/>				
Social Media - Web 2.0 Policy				

U.S. Department of Commerce
Office of the Chief Information Officer
Policy on the Approval and Use of
Social Media and Web 2.0 (SM/W2.0)

Why This Policy Is Necessary

[Other Applicable Commerce Policies](#)

[Responsibilities of Chief Information Officers](#)

[General Guidelines for the Use of SM/W2.0 Technologies in an Official Capacity](#)

[General Guidelines for the Use of SM/W2.0 Technologies in an Unofficial Capacity-
Responsibilities of Commerce Employees](#)

[Applying for Official Social Media and Web 2.0 Accounts](#)

[Specific IT Security Guidelines for Using Social Media and Web 2.0 Technologies](#)

[Resources for Additional Information](#)

Why This Policy Is Necessary

The Department of Commerce is committed to operating in an open and transparent way in all its communications and transactions with individuals and organizations. Social media and Web 2.0 (SM/W2.0) services are an increasingly important way for Commerce to interact in an efficient, effective, and transparent manner with all those who are affected by or have an interest in Commerce programs and activities.

SM/W2.0 services use many technologies, including XML feeds, wikis, blogs, social networking sites, discussion forums, collaborative research Web sites, comment features on news and video Web sites, and other mechanisms. Social media services allow the user to interact

directly with the Web site or other users. The result is that Web users are able to communicate simultaneously, directly, and instantaneously with all other users on the Web site. Commonly used social media services include YouTube®, Flickr®, Facebook®, MySpace®, and WordPress®.

SM/W2.0 technologies also present new and unprecedented challenges to the security of the information technology (IT) networks and systems that Commerce and its operating units use, as well as the privacy of personally identifiable information (PII) Commerce maintains. Commerce and other Federal information systems are targeted by persistent, pervasive, and aggressive threats. The threats may be directed against the network or system infrastructure, the records or information in the system, especially PII or other sensitive information. IT security controls currently in place may effectively protect Commerce information systems as presently configured, but the rapid development of Web 2.0 technologies and their emerging capabilities and uses present new and ever increasing risks that require continuing vigilance by IT security personnel and employees who use SM/W2.0 services.

The purpose of this policy is to provide guidance for operating units and Commerce employees to take full advantage of SM/W2.0 technologies while, at the same time, protecting Commerce and its employees by mitigating the risks inherent in using these services without the proper safeguards.

This policy conforms to and implements the following:

- [Guidelines for Secure Use of Social Media by Federal Departments and Agencies](#) that were adopted by the Chief Information Officers (CIO) Council and issued in September 2009.
- [President's Memorandum on Transparency and Open Government](#), January 21, 2009, calling for openness in Government and the establishment of a system of transparency, public participation, and collaboration.
- Office of Management and Budget (OMB) [Memorandum M-10-23](#), Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010.
- National Archives and Records Administration (NARA) [Bulletin 2011-02](#), Guidance on Managing Records in Web 2.0/Social Media Platforms, October 20, 2010.

Other Applicable Commerce Policies

The use of SM/W2.0 services must conform to other applicable Commerce policies, including the following:

- Department Administrative Order (DAO) 219-1, [Public Communications Policy](#), April 30, 2008, provides guidance for employees for communicating with the public about Commerce programs and activities and describes the role of the Office of Public Affairs (OPA) in ensuring that public communications are full, open, and accurate.
- [Web Policies and Best Practices](#) developed by the Commerce Web Advisory Council and

adopted by the Commerce CIO and Director of Public Affairs for implementation Commerce-wide, provide general guidance and requirements for the display of content on the Web.

- Commerce [Internet Use Policy](#), December 19, 2008, provides general guidance regarding Internet use by Department of Commerce personnel who are authorized to use Commerce resources.

Responsibilities of Chief Information Officers

Before any SM/W2.0 service or technology is approved for use on any Commerce network or system, the responsible operating unit Chief Information Officer (CIO), using established risk management methodologies, must conduct a risk-based assessment to determine whether the users in the operating unit should be allowed to access the particular SM/W2.0 technology, and whether any limitations on access or usage are warranted. The risk assessment should be conducted in accordance with the risk management principles in [NIST Special Publication 800-30](#), Risk Management Guide for Information Technology Systems, and other [NIST Publications](#) that apply. Additional guidance for CIOs is in the [Guidelines for Secure Use of Social Media by Federal Departments and Agencies](#).

The risk assessment conducted by a CIO applies only to the operating unit for which the CIO is responsible. Depending on the level of IT security measures in place, a SM/W2.0 service may be approved for use on one operating unit network or for access from one operating unit system but not others. Each CIO is responsible for maintaining a current inventory of SM/W2.0 technologies approved for access from their operating unit network(s) and systems.

Before authorizing employees to post information on a social media site, the CIO must verify that the SM/W2.0 service provider terms of service agreement has been approved by the Department of Commerce. Approved service agreements are on the Commerce Web Advisory Council [Social Media Web site](#).

The CIO may allow employees to access a site for which there is not an approved terms of service agreement provided that the service provider does not require users to agree to a terms of service agreement for access to the site.

[OMB M-10-23](#) requires agencies to conduct a Privacy Impact Assessment (PIA) in all situations in which any personally identifiable information (PII) will become available to the agency. OMB M-10-23 also requires agencies to post specialized privacy notices on the SM/Web 2.0 service itself, to the extent possible, and update agency privacy policies. Each responsible operating unit CIO must coordinate these activities with the Departmental Chief Privacy Officer (CPO).

The Commerce CIO is responsible for oversight and monitoring of implementation of this policy by operating unit CIOs.

General Guidelines for the Use of SM/W2.0 Technologies in an Official Capacity

The following are general guidelines for Department employees assigned official responsibility

for operating an official account or contributing to a SM/W2.0 Web site, whether that site is hosted internally by the Department (or an operating unit) or an external commercial service, on behalf of the Department or an operating unit.

- Department employees using SM/W2.0 technologies in an official capacity must do so only on Department-approved accounts and may only use official e-mail or other contact information for the creation and management of those accounts. In addition to helping the Department keep track of how many accounts it has, using Department-approved accounts will ensure that the Department knows who is responsible for each account it uses. In the case of services that do not require accounts for the creation of a Department presence, employees should follow the service-specific guidance available on the Commerce Web Advisory Council's [Social Media Website](#).
- In general, Department employees may only post from Department-approved accounts information that represents official agency positions (i.e., not personal opinion). However, if a posting concerns a fundamental research communication as defined by the Department's [Public Communications Policy](#) (DAO 219-1) and the posting is likely to be misinterpreted as an official Department position, Department employees must clearly state that they are providing their own personal opinions and not those of the operating unit, the Department, or the Federal Government.
- Department employees should conduct themselves in a professional, courteous, and honest manner in all public communications about or related to their Government work, whether on-line, in person, at public meetings, or in other settings.
- When posting a comment related to Department work to a public Web site, Department employees must identify themselves with their Department affiliation and/or official title.
- Posted information should be as accurate as possible. Although there is often a tradeoff between speed of communication and accuracy, employees speaking in an official capacity should take reasonable steps to ensure that the information that they provide is correct, and whenever feasible, to correct inaccurate information about Department work (especially on Department Web sites) that is brought to their attention.
- Department employees may not post any personally identifiable information on an SM/W2.0 Web site unless the information would otherwise be released consistent with the [Privacy Act](#) and [Freedom of Information Act](#) (FOIA). Questions concerning whether employees may release PII may be directed to the CPO or the operating unit FOIA Officer. The improper release of PII or other sensitive information may result civil or criminal penalties, in accordance with the Privacy Act.
- Department employees may not improperly use or post materials protected by copyright, trademark, patent, trade secret, data rights, or related protections for intellectual property. Proper use may require obtaining written permission from the owner of such information. The Department's Office of the General Counsel can assist

employees in obtaining these permissions when necessary. Additionally, employees should exercise diligence with respect to the Department's and their operating unit's intellectual property, in logos, slogans, trademarked names, etc. Employees should not encourage or allow third-party use of Departmental emblems or logos without approval, in accordance with [DAO 201-1](#), Approval and Use of Seals, Emblems, Insignia and Logos.

- Department employees may not include surveys, polls, questionnaires, etc., on official SM/W2.0 Web sites unless the questions have received Office of Management and Budget (OMB) Paperwork Reduction Act clearance. The [Paperwork Reduction Act](#) (PRA) prohibits certain information collections by the Department without prior approval by OMB. While OMB has determined that some uses of social media are not considered information collection under the PRA, please contact the General Law Division to determine if the PRA applies to a specific use.
- Department employees use of SM/W2.0 services should not include requests to contact a member of Congress, a jurisdiction, or an official of any Government (Federal, state, or local) to favor or oppose any legislation, law, or appropriation because these activities are prohibited by the Anti-Lobbying Act.
- Department Web sites, pages, etc. that contain postings and/or responses by the public require diligent monitoring. Operating units using SM/W2.0 technologies must prevent the posting or immediately delete postings that contain:
 - o comments regarding a political party or a candidate in a partisan political campaign (which is a campaign in which candidates are identified by political party);
 - o requests to contact a Member of Congress or official of any government, to favor or oppose any legislation, law, or appropriation;
 - o advertisements, endorsements, or promotions; and
 - o vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups.

Because such monitoring and filtering might give rise to public criticism, operating units are required to use either the Office of the Secretary's comment policy or develop and post their own comment policy approved by their Office of General Counsel.

- Department employees are prohibited by the [Hatch Act](#) from engaging in political activity on Government premises or using Government resources. Political activity includes any activity directed toward the success or failure of a political party or a candidate in a partisan political campaign.
- When posting information using SM/W2.0 technologies, agencies should ensure and maximize the quality, objectivity, utility, and integrity of posted information (including statistical information), and ensure that measures are in place to allow for the correction of information not meeting that standard. This is required under the Department's

Information Quality Act Guidelines.

- Agencies are required to ensure that people with disabilities or limited English proficiency have an accessible version of official content posted online, in compliance with [Section 508 of the Rehabilitation Act of 1973](#), and [Executive Order 13166](#), Improving Access to Services for Persons With Limited English Proficiency. Materials posted to SM/W2.0 services also must be posted in accessible formats on the official Department Web site; non-governmental SM/W2.0 sites may not be the sole location where content is posted. This will ensure that people with disabilities, or who have limited English proficiency, always have an accessible version of the content and that the official version of the content is located on a Department Web site.

If the SM/W2.0 technology allows the public to respond to official postings, the Department Web site must also provide visitors with the ability to communicate with the Department so that members of the public do not have to register with or provide personal information to third-party Web sites that may require registration or the provision of personal information. The Department Web site must provide an alternative way, e.g., e-mail address for members to communicate directly with the Department without providing personal information to a third-party Web site.

- Department employees may not solicit consensus advice from the public using SM/W2.0 technologies. The [Federal Advisory Committee Act](#) prohibits agencies from receiving consensus advice from *de facto* committees or groups that arise outside of the structure and public scrutiny of a formally established advisory committee.

- Operating units must ensure that the content maintained on their SM/W2.0 sponsors' Web sites, especially PII and other sensitive information, is secure and adequately safeguarded from unauthorized disclosure or destruction. The records must be retained consistent with the Department's [records retention requirements](#). NARA [Bulletin 2011-02](#), Guidance on Managing Records in Web 2.0/Social Media Platforms, provides additional guidance.

- Operating units interacting with the public through SM/W2.0 technologies must ensure that such interactions require and generate the least amount of PII possible from their users. To that end, and whenever feasible, operating units must edit and actively manage their SM/W2.0 Web site or application settings to make sure that only the minimum amount of PII necessary to effectively use such technologies is being generated/collected. OMB Memorandum M-10-23 establishes requirements for a PIA, which must document the agency's decision process. Agencies should discuss these details as appropriate in the privacy notice posted to the SM/W2.0 technology, as described in OMB Memorandum M-10-23.

- When visitors to an official Department Web site are redirected from the Department site to a third-party site, the visitors must be notified that they are leaving the official agency site, e.g., when a visitor to a Commerce site is redirected to view a video on YouTube®. Further, Department employees' use of links to such third-party sites must be consistent with their operating unit's linking policy. This is required by OMB Memorandum [M-05-04](#), Policies for Federal Agency Public Web Sites, and OMB

Memorandum [M-10-23](#), Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010. .

- The Department may not rely on SM/Web 2.0 social media as the exclusive means of distribution of information. Materials posted to SM/W2.0 services also must be posted on official Government Web sites, *and* alternative, non-electronic forms of information must be made available upon request, pursuant to OMB [Circular A-130](#), Management of Federal Information Resources.
- The Department does not endorse commercial products or services. Department employees should not post third-party advertisements or otherwise engage in activities that might lead to a conflict of interest, appearance of endorsement, affiliation, or authorization, or otherwise lead the public to believe that your operating unit supports the views, products, services, etc. of third-parties.
- Department Web sites must not collect any personal information from children (under the age of 13) in violation of the [Children's Online Privacy Protection Act](#).

General Guidelines for the Use of SM/W2.0 Technologies in an Unofficial Capacity - Responsibilities of Commerce Employees

The following are general guidelines for Department employees' unofficial or personal use of SM/W2.0 technologies. The safe and legally appropriate use of SM/W2.0 services and technologies involves behavioral issues, as well as technology issues. It is essential that employees adhere to the following requirement. Employees should be aware that their operating unit CIO may not allow access to certain SM/W2.0 services. Please note that these guidelines for unofficial or personal use do not apply to Department contract employees, except to the extent that they are using Department resources to provide information to the public.

- Pursuant to the Department's [Public Communication Policy](#) (DAO 219-1), Department employees on Government or non-Government Web sites, who wish to post or upload material using SM/W2.0 technologies that relates to the programs or operations of their operating unit and that is related to their official duties, must submit their communication for review to their supervisor or a public affairs officer at their operating unit. If a posting concerns a fundamental research communication as defined by the policy, employees should clearly state that they are providing their own personal opinion and not that of the operating unit, the Department, or the Government.
- Employees should be mindful of blurring their personal and professional life when using SM/W2.0 technologies. Employees should not establish relationships with working groups or affiliations that may reveal sensitive information about their job responsibilities.
- Although Department employees are encouraged to learn about and experiment with these tools in an unofficial capacity, they should be mindful that any information posted

on the Web, even when on-site privacy controls are used on SM/W2.0 sites, could become public.

- Do not use your Federal job title when you are using social media in a personal, unofficial capacity to avoid any confusion about whether you are communicating in an official capacity. You may use your title when it is self-evident that you are not posting in an official capacity, such as posting a resume or listing your employment history on a social network profile.
- Do not disclose any information obtained on the job that is not already publicly available. This includes national security (classified) information, personally identifiable information, proprietary or business confidential information, pre-decisional information, or similar sensitive information. Avoid establishing relationships or affiliations with groups that are not appropriate or that may result in the inadvertent sharing of non-public sensitive information.
- The [Hatch Act](#) prohibits Federal employees from soliciting, accepting, or receiving campaign contributions, including through the use of SM/W2.0 technologies. This prohibition includes hosting or posting to a Web site that includes a link for making contributions to a political party or a candidate in a partisan election, that is, a campaign in which candidates are identified by political party. Additional information is available from the OGC [Ethics Law and Programs Division](#) Web site, by phone at 202-482-5384, or via e-mail at ethicsdivision@doc.gov.
- The Commerce [Internet Use Policy](#) allows employees to use their Government computer and SM/W2.0 for their personal use, provided that access is allowed by the operating unit CIO and use of equipment is minimal. Additionally, use of SM/W2.0 must not interfere with office operations or involve commercial activities (profit-making or business), partisan political activities, or sexually explicit communications.
- Remember that information posted on SM/W2.0 sites is available to a wide audience of users. How you present yourself on these Web sites will reflect on Commerce and the Federal Government.
- Department employees are allowed to use their Government computer for limited personal use (as per the Department [Internet Use Policy](#)), provided that use of equipment is minimal, does not interfere with office operations, and does not involve commercial activities (profit-making or business), partisan political activities, or sexually explicit communications.

Applying for Official SM/W2.0 Accounts

Commerce employees should consult the list of Commerce approved [Social Media and Web 2.0 Web sites](#) and use the Web-based [Commerce Social Media Application](#) to apply for SM/W2.0 accounts.

Specific IT Security Guidelines for Using SM/W2.0

Technologies

SM/W2.0 present IT security challenges beyond those of static Web sites, and it is essential to adhere to applicable Federal and Department IT security requirements, including the following:

- The Administrative Point of Contact (APOC) for a SM/W2.0 account should be solely responsible and accountable for the administration, password control, and access management of the account.
- APOCs should not use the same password for more than one account. Many SM/W2.0 sites allow account administrators to assign administrative rights to other users. When available, this feature should be used instead of sharing passwords.
- Browsing should be performed from non-administrative accounts, and browsers should be configured in a secure manner.
- Even in cases where SM/W2.0 Web sites do not enforce strong password requirements, strong passwords should be used in accordance with [CITR-009: Password Requirements](#) for password length, expiration, and complexity, e.g., use of upper and lower case letters and special characters.
- APOCs must not use the same password for logging in to their Commerce or operating unit network that they use to access any SM/W2.0 site. Failure to use different passwords could compromise the security of the Commerce or operating unit network.
- APOCs should only follow links and download files from known and secure sources. Any file downloaded from a SM/W2.0 site must be virus scanned before opening. Upon receipt of a suspicious message, link, or file to download from a known person, APOCs should verify that the item was actually sent by the person before virus scanning and opening it.
- SM/W2.0 accounts must be monitored on a regular basis. In the event pages are hacked or defaced, a report must be sent immediately to [DoC Computer Incident Response Team \(CIRT\)](#) or the operating unit's IT Security Officer. After reporting the incident, the APOC for the account must contact the software or service provider to regain control of the account and restore the page. Passwords will be changed immediately after any hack or page defacement.

Resources for Additional Information

- Office of the General Counsel, [General Law Division](#) (202-482-5951 or epackard@doc.gov).
- Office of the General Counsel, Ethics Law and Programs Division (202-482-5384 or ethicsdivision@doc.gov).
- Diana Hynek, Office of IT Policy and Planning, OCIO (202-482-0266 or dhynek@doc.gov).

- Mike Kruger, Director of New Media, OPA (202-482-2556 or mkruger@doc.gov)
- Jonathan R. Cantor, Chief Privacy Officer and Director of Open Government (202-482-3463 or jcantor@doc.gov)
- Dan Rooney, Records Management Officer, OCIO (202-482-0517 or drooney@doc.gov)

Date of policy superseded: None

Revision status: None

Approved by Simon Szykman, Chief Information Officer, 12/09/2010

Questions regarding this section may be directed to the [IT Policy, Guidance & Legislation Administrator](#)

U.S. Department of Commerce | Privacy Policy | FOIA | USA.gov | No FEAR Act | Disclaimer | Feedback |
Forms | Information Quality