



## FEMA Web 2.0 Policy

---

### **I. Purpose**

Provide initial guidance regarding the use of emerging Web technologies to improve the Federal Emergency Management Agency's (FEMA's) communication with stakeholders, internal communication, and collaboration. (This policy includes, but is not limited to, all social media materials, e.g., Twitter, Facebook, and YouTube.)

The Directive follows the standards and guidelines for Federal government web usage and complies with the Department of Homeland Security (DHS) and FEMA policies. It ensures that FEMA is harnessing new technologies and makes Government transparent, participatory, and collaborative. This Directive is effective as of the date of signature and will be reviewed annually.

It provides a framework to maintain organizational functions and uphold regulatory and legal compliance for official FEMA use. Certain policies included in this Directive delineate responsibilities and processes to be followed by selected directorates or offices; others dictate general compliance for and expectations of Web 2.0 use by appropriate individuals, offices, and/or directorates.

### **II. Scope**

This Directive is intended for all FEMA employees, staff, offices, directorates, and supporting personnel using or considering use of Web 2.0 technologies in an official capacity.

### **III. Background**

"Web 2.0" refers to Web applications that facilitate and foster interactive information sharing, interoperability, and collaboration on the Internet, allowing users to interact with each other and serve as contributors to the website's content. Examples of Web 2.0 tools that exist in the private sector include social networking, video-sharing, wikis, and blogs.

The Agency endorses the secure use of Web 2.0 tools to enhance external communication, internal collaboration, and communication with stakeholders. Web 2.0 technologies have the ability to increase information exchange, streamline processes, and foster productivity improvements across the Agency in these three categories. The Agency will carefully consider the various types of tools and select those that are appropriate for Agency needs and the security environment. This Directive outlines the measures and procedures needed to ensure compliance with laws and regulations that govern the Agency's online activities.

Operating procedures regarding the use of Web 2.0 components are promulgated by the Office of External Affairs for public facing websites and by the Office of the Chief Information Officer (OCIO) for non-public facing websites in consultation with the Office of Chief Counsel (OCC), the Privacy Office, and the Records Management Division.

#### IV. Policy and Procedures

The process to establish a FEMA-authorized Web 2.0 application will depend on whether the tool will be hosted on a Government-operated server and website or on an external Federal Information Security Management Act (FISMA)/508-compliant server (outside of a Government firewall).

The general process to establish either a FEMA-hosted or a non-FEMA-hosted application follows similar criteria. Important considerations, such as cyber-security risks posed by on-network applications, will be of greater concern to participating FEMA stakeholders. Because of the legal and security restraints of Federal agencies, the following policies apply to all use of the Web 2.0 product by FEMA programs.

A. All public facing Web 2.0 technology must be authorized by the Office of External Affairs in consultation with:

1. OCC
2. Cyber Security Information Officer (CSISO)
3. Records Management
4. Privacy Office
5. FEMA OCIO (if a new application is being purchased)

Failure to receive authorization from External Affairs will result in the IT Security Branch's blocking all FEMA access to the unauthorized Web product.

B. All non-public facing Web 2.0 technology must be authorized by the Chief Information Officer (CIO) in consultation with:

1. OCC
2. CISO
3. Records Management
4. Privacy Office
5. FEMA OCIO (if a new application is being purchased)

Failure to receive authorization from the OCIO will result in the OCIO's removing the product from the FEMA network.

C. All third party Web 2.0 technology must have a Terms of Service or license agreement that has been reviewed and approved by OCC.

D. FEMA may not use on a DHS/FEMA contractor server any Web 2.0 product that uses tracking technology unless it is in compliance with OMB Memorandum 10-22.

E. All FEMA Web 2.0 products must contain a comment policy written in consultation with OCC. Posted comments must be relevant and must not contain racist, sexist, discriminatory, or foul language; privacy information; malicious links; or non-public information.

F. In compliance with the comment policy, FEMA must moderate all comments posted using Web 2.0 products prior to posting if technologically possible. If it is not technologically possible, the comments must be monitored by the sponsoring program at least three times a day.

G. If technologically possible, Web 2.0 products must allow for anonymous posting. FEMA will not use any Web 2.0 products on its public facing sites that require a user to give his or her full

name and/or email address. FEMA may not use third party products where the only purpose of the product is to obtain public feedback (no information is being presented to the public) that are hosted on the third party product's site (unless that site is a FEMA contractor) that require a log in to post. FEMA may not use a third party product that requires a user to pay for access to Government information.

- H. Web 2.0 products may not link to non-Government websites or products unless there is a mission-critical need to do so. If there is a mission-critical need to link to a non-Government product, the link should be made to the specific mission-critical content. The content should have limited commercial activity and should not imply an endorsement of any product or organization. If technologically possible, language should be included on a Web 2.0 product to disclaim any endorsement of non-Federal organizations or their products and services.
- I. FEMA may not link in any way to commercial entities other than media entities; individuals, unless the individuals are Federal, State, or local government employees acting in their official capacity (not for their campaign); or non-profits unless the organizations are members of the FEMA Voluntary Organizations Active in Disaster (VOAD) list, the organizations are Citizen Corps Affiliates, or if there is a mission-critical need to do so.
- J. All FEMA-produced content on third party websites, including videos and photos, must be available on a FEMA public website.
- K. All Web 2.0 products on public facing sites must be branded in accordance with the branding guidelines established by the Office of External Affairs.
- L. FEMA must obtain a Government use license for any non-Federal Government content other than links or comments posted on FEMA Web 2.0 products.
- M. All Web 2.0 content is a Federal record and must be retained per the Federal Records Act and National Archives and Records Administration (NARA) and FEMA records schedules. If a records schedule has not been created for the Web 2.0 content, the sponsor of the Web 2.0 product must retain all content until a records schedule is created and the content may be disposed of per the schedule. FEMA must retain control of all of its records and may not store them on third party products not under contract with FEMA to provide storage of records.
- N. All FEMA program sponsors will act impartially toward third party Web 2.0 technology. If multiple third party products may be used to accomplish the same mission goal, the sponsoring program must use all approved Web 2.0 products within time, budget, and manning constraints. For example, a program may not use Facebook without also using other approved tools that can accomplish the same goal.
- O. FEMA will not use Web 2.0 technology to conduct surveys or to ask questions that collect information from non-Federal employees without approval from OMB. FEMA programs may ask general questions such as "what do you think?" or "screen name."
- P. No FEMA employee will post any non-publicly releasable information on any public facing Web 2.0 product. Unless authorized by External Affairs, employees may not speak for the Agency or discuss the intricacies or development of Agency policies or programs unless the disclosure is protected by the Whistleblower Protection Act.
- Q. External Affairs will maintain a list of public facing Web 2.0 products on FEMA.gov. The list will include a disclaimer of any endorsement of non-Federal products and organizations and a statement of impartiality for products not in use by FEMA with an email address to contact the Agency about products.

- R. Web 2.0 products that are not public facing but are accessible to non-FEMA employees must contain rules of behavior, written in consultation with OCC, to which users must agree. These rules must include a statement prohibiting the release of non-publicly releasable information.
- S. FEMA may not use Web 2.0 technology to seek continual consensus, recommendations, or advice from non-Federal, State, or local government officials acting in their official government capacity except using technology that is open to the general public for comments.
- T. All Web 2.0 products require legal review by OCC, which provides advice and guidance to the product owner.
- U. Employee Use of Web 2.0
  - 1. An employee may use Web 2.0 applications on his or her own time. This implies that the employee will not engage in personal Web 2.0 use at his or her workplace during business hours and will not use Government equipment for personal Web 2.0 use.
    - a. There is a limited personal use exception that allows for the use of Government equipment, but it is limited to authorized use during “employee use in personal time.”
    - b. “Employee use in personal time” means times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use Government office equipment during their own off-duty hours, such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times).
  - 2. In general, an employee may not state or imply that his or her personal use of Web 2.0 applications is official.
  - 3. During personal use, employees are discouraged from engaging in social media to respond to discussions about FEMA (even if erroneous or slanderous). This is the role of External Affairs, which has the responsibility of presenting a unified and on-target message for all of FEMA.
  - 4. Any employee who makes a public comment without prior authorization to speak officially for FEMA or while off-duty must disclose his or her relationship to FEMA (i.e., employee) and acknowledge that his or her response is not reflective of official FEMA policy, actions, etc. This requirement does not apply to social media interactions that are strictly personal, meaning the subject matter of the exchanges, public or private in nature, does not pertain to topics or issues relating to FEMA.
    - a. Referencing official FEMA statements or policy available to the public (i.e., by linking to a FEMA press release on FEMA.gov) is permissible and recommended, as appropriate and applicable.
  - 5. If an employee encounters a situation, either in an office location or in the field, in which public comment from FEMA appears warranted and the employee does not have prior authorization to communicate official FEMA information to the public or media, the employee should contact the appropriate local, State, tribal, regional, or Federal FEMA external relations representative.
  - 6. An employee may not release or discuss any non-public Government information as defined by Title 5, Code of Federal Regulations (CFR), Section 2635.703. Employees are free to discuss all public Government information, share all public information, and refer users to Government websites for additional guidance if it is available.

7. An employee may not use his or her Government email account for the personal use of Web 2.0 applications.
8. An employee may not send Web 2.0 personal correspondence to a Government email account for any purpose, including, but not limited to, invitations, chatting, and archiving.

## V. Responsibilities

- A. The Office of External Affairs, shall:
  1. Oversee all external communications on publicly accessible sites.
  2. With OCIO, edit, revise, amend, or otherwise maintain this Directive according to its review guidelines.
- B. The Office of Policy and Program Analysis, shall provide leadership, analysis, coordination, and decision-making support on Agency policies, plans, and key initiatives relating to websites and content.
- C. The Information Technology Branch, OCIO, shall provide guidance on IT risks, challenges (including cyber-security, etc.), and possible resolutions for issues relating to FEMA use of Web 2.0 technologies/applications.
- D. The Records Management Division and the Privacy Office, shall provide guidance and validate compliance of Web 2.0 technologies relating to privacy issues and records management.
- E. The Office of Chief Counsel (OCC), shall:
  1. Provide legal counsel for all technology-related initiatives.
  2. Identify legal challenges and possible resolutions.
  3. Validate that all use of Web 2.0 is legally compliant with pertinent laws and regulations.
  4. Negotiate any amendments to Terms of Service Agreements.
- F. Web Sponsors (or users, including offices and directorates), are responsible for overall compliance with all aspects of this Web 2.0 policy. Accordingly, Web Sponsors are also responsible for all budget, implementation, personnel, management, authorization, and content matters related to use of Web 2.0 technologies. The content owners on those sites and products are responsible for ensuring they conduct a reasonable review of the material to determine if there is any non-publicly releasable information, privacy information, or other restricted content being made available on their sites.

## VI. Authorities

- A. The Clinger-Cohen Act of 1996, Public Law 104-106, Title 41, United States Code (U.S.C.), Section 251 note, dated February 10, 1996.
- B. The E-Government Act of 2002, Public Law 107-347, 44 U.S.C. § 101 note, dated December 17, 2002.
- C. 5 CFR Part 2635, "Standards of Ethical Conduct for Employees of the Executive Branch."
- D. Executive Order 13526, *Classified National Security Information*, signed December 29, 2009, codified at 75 Federal Register (Fed. Reg.) Page 707, dated January 5, 2010.
- E. Presidential Memorandum, *Transparency and Open Government*, issued January 21, 2009, codified at 74 Fed. Reg. 4685, January 26, 2009.

- F. OMB Circular A-130, *Management of Federal Information Resources*, Revised Transmittal Memorandum No. 4, dated November 28, 2000.
- G. OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, dated September 26, 2003.
- H. OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, dated June 25, 2010.
- I. OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, dated June 25, 2010.
- J. DHS Management Directive (MD) 0007.1, *Information Technology Integration and Management*, dated March 15, 2007.
- K. DHS MD 0470.2, *Privacy Act Compliance*, dated October 6, 2005.
- L. DHS MD 4300A *DHS Sensitive Systems Policy Handbook*, dated August 9, 2010;  
<http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/sspolicy.aspx>
- M. DHS MD 4400.1, *DHS Web (Internet, Intranet, and Extranet Information) and Information Systems*, dated March 1, 2003.
- N. DHS MD 11042.1, *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*, dated January 6, 2005.
- O. FEMA Directive 136-2, *Web Site Development and Maintenance*.

**VII. Responsible Office**


Office of External Affairs

**VIII. Supersession**

This is a new Directive.

**IX. Questions**

Questions or concerns regarding this Directive should be directed to the Integrated Communications Branch Chief in the Public Affairs Division, External Affairs Office, at 202-646-4600.

  
\_\_\_\_\_  
Brent Colburn  
Director  
Office of External Affairs

Date: 12/16/10