Interim Guidance on the Use of Social Media

Contents

1 Background

1.1 Definition of Social Media

Social media, sometimes also called Web 2.0, is a general term that encompasses various computer-mediated activities, including blogs, video and photo sharing, podcasts, social networking, and virtual worlds. Social media integrates technology, social interaction, and content to allow individuals and online communities to create, organize, edit, comment on, combine, and share content and ideas. Social media services use various Web-based technologies that provide strategic communication tools to enhance the flow of information to and from both the general public and specifically targeted stakeholder groups. The U.S. Nuclear Regulatory Commission (NRC) can make use of these services to enhance collaboration and transparency and broaden the agency's ability to demonstrate to audiences what the NRC does and why.

The social media services described in this interim guidance include both (1) commercially provided Web sites and online applications that are not exclusively operated or controlled by the NRC and (2) publically accessible Web sites and online applications that are operated and controlled by the NRC.

1.2 Document Purpose

The NRC is enabling the use of selected social media and Web-based interactive technologies such as blogs, wikis, and social networks as another way to enhance public and stakeholder participation in NRC activities and to enable NRC employees to network and interact with professional colleagues. This interim guidance describes how and when NRC employees may represent the agency or use agency assets to engage in social media activities and defines the NRC's expectations for conducting such interactions. This interim guidance also addresses Office of Management and Budget (OMB) M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies" (http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf) and OMB M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications" (http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf).

1.3 Benefits and Mission Alignment

The NRC is committed to openness and transparency and already uses a variety of ways to communicate with and engage the public, including public meetings, speeches, workshops, press releases, fact sheets, videos, the Agencywide Documents Access and Management System (ADAMS), the *Federal Register*, Webcasts, e-mail, the NRC Web site, and more. Social media provides another means for the NRC to engage the general public and specific stakeholder groups in its activities, since many people are increasingly using social media to obtain and share information.

The NRC also supports the use of social media to obtain feedback, engage in public discussions related to the agency's mission, and correct errors or misconceptions about the agency's activities.

2 Applicability/Responsibility

This document applies to all NRC employees. Unless explicitly stated as a condition of a contract, purchase order, or consultant agreement, NRC contractors or consultants are not authorized to use social media or represent the NRC. This document is not intended to alter or replace any existing laws, regulations, or policies.

2.1 NRC Employees

The relationship between the agency as an organization and an NRC employee is based on trust. Consequently, NRC employees are expected to be responsible for their own professional conduct.

2.2 Managers

Managers in offices with bargaining unit employees may use the Area Labor Management Partnership Council as a forum to engage with the bargaining unit employees designated by the National Treasury Employees Union on issues related to office usage of social media.

3 Social Media Categories of Use

This guidance often refers to "NRC employees' participation in social media activities." This phrase simply means the interactive exchange of information between NRC employees and the public via social media activities. All social media usage must be conducted consistent with existing rules of behavior governing NRC employees and existing records management policies, information assurance policies, and other policies related to agency representation in a public forum. Section 7 of this guidance lists the existing policies that are applicable to social media use by NRC employees.

As with any other interaction between the NRC employees and the public or professional organizations, participation can assume a few different forms:

- participation as an Authorized NRC Representative
- participation on official duty (but not as an official spokesperson for the NRC)
- participation in a private capacity (personal use)
- creation of an official NRC-sponsored social media site or account

3.1 Participation as an Authorized NRC Representative

The NRC may specifically select and designate NRC employees to represent the agency during participation in public social media activities when a significant agency interest would be served. Service as an Authorized NRC Representative with an outside professional organization's social media site does not connote agency agreement with or endorsement of that organization. Nominations for employees to serve as Authorized NRC Representatives must be approved by their office director or designee who will notify the Office of Public Affairs (OPA) of the employee's designation.

Employees designated as an Authorized NRC Representative must work to maintain consistency of messages as approved by their management (and in concert with OPA if

appropriate) when engaging in discussions, clarifying NRC positions, correcting errors, and undertaking other tasks as officials speaking for the agency. For example, an NRC subject matter expert on emergency management must work with OPA to clarify a new regulation on an industry blog or answer questions about protective measures on a forum for State emergency managers. Authorized NRC Representatives must understand and adhere to all relevant records management rules and must promptly report to management and OPA any online situation likely to cause media attention, negative public outcry, or other ramifications for the agency.

3.2 Participation while on Official Duty

The NRC permits NRC employees to participate in a social media activity while on official duty if the agency can derive a benefit from that person's participation and if the primary purpose of the activity contributes to professional knowledge in fields related to NRC work or to the collaboration with peers outside of the NRC.

This type of participation is akin to the use of Web sites and public resources on the Internet, the use of email and listservs, and participation in conferences and forums to increase professional knowledge and contribute to the performance of official duties. This type of participation could include networking with colleagues in other Federal agencies to discuss common problems, share best practices, and exchange ideas. NRC employees must adhere to all NRC policies for handling non-public information (e.g. sensitive, privacy related) when participating in a public social media activity to avoid potential disclosures. Such communications, while job-related, would not represent the NRC's official position or policy regarding the topics discussed, but they may represent the employee's professional opinion. For example, an NRC employee who participates in an online discussion forum for health physicists to discuss training best practices might share a training approach that he or she personally found useful.

This type of participation also includes the use of social media for learning and consuming information such as job related training, reviewing current events, and obtaining information directly related to and in support of one's job functions. For example, an NRC employee might watch an online training course or read the transcript of an industry workshop.

NRC employees who have questions on whether a specific use of social media is appropriate for participation on official duty should speak with their supervisors. Employee use of social media on official duty must be in compliance with Management Directive (MD) 2.6, "Information Technology Infrastructure."

3.3 Participation in a Private Capacity

The NRC permits employees to use NRC resources to participate in a private capacity in social media activities when such use is in compliance with MD 2.7, "Personal Use of Information Technology." The definition of "information technology" (IT) in MD 2.7 includes the use of public social media sites. As stated in MD 2.7, "it is the policy of the U.S. Nuclear Regulatory Commission to permit employees limited use of agency information technology for personal needs if the use does not interfere with official business and involves minimal or no additional expense to the NRC." While this interim guidance does not cover personal use, NRC employees are encouraged to understand the reach of social media and the unintended consequences that can occur when posting content in a public venue.

3.4 Creation of an Official NRC Sponsored Social Media Site or Account

The NRC may have an NRC official presence on a social media site by creating an NRC official account, dedicated channel, page, or other venue that clearly operates as an official platform for the NRC and promotes the agency's activities, mission, goals, positions, policies, and actions to the general public. Such a presence is akin to using the NRC Web site (http://www.nrc.gov) as a central portal for the public to find information on all aspects of the agency. An example would be creation of an official NRC blog page or official NRC YouTube channel.

OPA establishes NRC official sites/accounts and oversees the use of social media services used for NRC official communication. In coordination with OPA, NRC offices may designate authorized NRC employees to directly post content on these services. Similar to the process used for managing the NRC Web site, this allows the agency to establish a single point for the public to interact with the NRC on specific social media services, while allowing for the decentralized posting and management of content. In some cases, individual NRC offices may create their own accounts, with OPA permission. For example, an NRC office might wish to establish an office-level Twitter account that provides information to a very specific and unique set of stakeholders.

4 Guiding Principles

Whether one is using social media for participation as an Authorized NRC Representative, participation while on official duty, or creation of an official NRC-sponsored social media site or account or otherwise using NRC assets, users should be aware of several principles:

- NRC employees are expected to know and follow agency and executive branch conduct guidelines, such as Title 5 of the *Code of Federal Regulations* (5 CFR) Part 2635, "Standards of Ethical Conduct for Employees of the Executive Branch" (see http://www.usoge.gov/laws_regs/regulations/5cfr2635.aspx) and 5 CFR Part 5801, "Supplemental Standards of Ethical Conduct for Employees of the Nuclear Regulatory Commission" (see http://www.access.gpo.gov/nara/cfr/waisidx_02/5cfr5801_02.html).

- NRC employees must not engage in vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups.

- NRC employees must not endorse, oppose, or contribute to any partisan parties, candidates, or groups.

- NRC employees must respect copyright and trademark laws, as applicable.

- NRC employees are expected to conduct themselves professionally in the workplace and to use agency IT for activities that are appropriate to the agency's mission. The handbooks for MD 2.6 and MD 2.7 list activities the NRC considers to constitute misuse or inappropriate personal use of agency IT resources.

- NRC employees are expected to comply with all Computer Security Office mandatory computer security policies, standards, procedures, processes, and templates (see MD 12.5, "NRC Automated Information Security Program"). This includes the "NRC

Agency-wide Rules of Behavior for Authorized Computer Use" (ADAMS Accession No. ML082190730).

- NRC employees must protect, as necessary, sensitive information such as Sensitive Unclassified Non-Safeguards Information, Safeguards Information, and classified information (see "Sensitive Unclassified Non-Safeguards Information (SUNSI) Handling Requirements"; MD 12.2, "NRC Classified Information Security Program"; and MD 12.7, "NRC Safeguards Information Security Program").

- NRC employees are expected to maintain a clear and distinct separation between personal opinion and official NRC information. If a personal profile identifies an individual as working for the NRC, or if an NRC employee has a public-facing position such that the general public would know the individual's NRC affiliation, the NRC employee should ensure that his or her profile and related content (even if they are of a personal and not an official nature) are consistent with how he or she wishes to present himself or herself as an NRC professional, are appropriate with the public trust associated with his or her position, and conform to existing standards (e.g., 5 CFR Part 2635).

- NRC employees who notice inappropriate, misleading, or inaccurate information about the NRC while engaged in social media activities are encouraged to notify either OPA or an employee designated as an Authorized NRC Representative. NRC employees who are not Authorized NRC Representatives should not take direct action (such as posting a rebuttal to the incorrect information) but should refer the matter as directed above.

- NRC employees should be aware that documentary materials created, received, or accessed when using social media may need to be maintained as Federal records in accordance with the policies and procedures set forth in MD 3.53, "NRC Records and Document Management Program."

5 Authorized and NRC Sponsored Social Media Representation

Any social media activities involving participation as an Authorized NRC Representative or creation of an official NRC-sponsored social media site or account must also adhere to the following nine rules:

(1) OPA creates and maintains social media service account profiles for NRC official presence sites, such as the NRC Blog page or NRC YouTube channel page. In some cases, with OPA permission, individual NRC offices may create their own profiles. For example, an office may wish to establish an office-level Twitter account that provides information to a very specific and unique set of stakeholders.

Individual NRC offices may initiate and maintain profiles necessary to fulfill their designated representation responsibilities, such as registering for a forum in order to post information, according to their office's social media guidance.

When establishing accounts/profiles for authorized and NRC sponsored social media representation and use, NRC employees must ensure the following:

– The profile complies with NRC computer security policy, standards, and guidance available.

– The user's username is not an NRC account username (e.g., the user's NRC network identifier), should not reflect personal information about the user, and must be approved by the office director or designee (see MD 12.5).

– The profile information, such as user's biography, is approved by the office director or designee and must reflect NRC-relevant information that is not sensitive.

– The profile is linked to the user's NRC e-mail account (John.Doe@nrc.gov), not to a personal account.

– The authorized NRC accounts/profiles are restricted to NRC employee work and office-related information only, and no personal information, including personally identifiable information (PII), is permitted.

– The authorized NRC profile displays only images approved by the office director or designee.

(2) NRC official presence on social media services should function similarly to the NRC Web site. The information, whether print, audio, or video, should be accurate, timely, and appropriate. It should be appropriately reviewed and approved internally before dissemination. It should serve to better inform the public about the NRC's activities, policies, practices, actions, responsibilities, or mission. Information on an NRC official presence site should clearly be identified as official NRC information and must adhere to all existing MDs related to Web postings or public meeting presentations. A mechanism also needs to be in place to periodically check posted information for ongoing usefulness and accuracy and to update or remove content that is no longer timely, relevant, or correct. Information posted on social media services on an NRC official presence site must be specifically approved by OPA or, by agreement, posted by authorized NRC employees in each office.

(3) If NRC posts a link that leads to a third-party website or any other location that is not part of an official government domain, the NRC must provide an alert to the visitor explaining that visitors are being directed to a nongovernment website that may have different privacy policies from those of the NRC.

(4) Information posted by authorized NRC employees must clearly reflect that the content is an official NRC communication and not simply an employee's opinion. Information posted on social media services by designated representatives is controlled by office directors or designees, who set the office-level procedures and identify subject matters experts who can provide official NRC content. Office directors or designees are expected to include OPA notification in their office-level procedures, especially when the content may lead to media or congressional inquiries, consistent with MD 5.5, "Public Affairs Program." Reuse of existing content (e.g., posting a paragraph from an NRC brochure to a social media service) should not need additional content review.

(5) Information disseminated or collected through social media activities that meets the definition of a Federal record must be in compliance with the Federal Records Act (see 44 U.S.C. Chapter 31 at http://www.archives.gov/about/laws/fed-agencies.html), National Archives and Records Administration regulations (see http://www.archives.gov/records-mgmt/bulletins/2011/2011-02.html), and MD 3.53 and related guidance and processes.

In addition, this information may also need to be retained to satisfy the NRC's obligations pursuant to the Freedom of Information Act (see MD 3.1, "Freedom of Information Act") or to accomplish discovery in agency litigation.

(6) Comparable information disseminated to the public through social media services must be available to the public via an alternative official agency means. If public information, such as public feedback, is collected through social media services, the NRC must have an alternative official agency means to collect public information that does not involve social media, such as the NRC public website.

(7) Use of social media services must be in compliance with the Paperwork Reduction Act of 1995 (see 44 U.S.C. 3501 et seq (Public Law 104-13) at http://www.archives.gov/federal-register/laws/paperwork-reduction/). For example, OMB must approve Web surveys (including popups), online focus groups, questionnaires, and any solicitation of responses to identical, specific questions before their posting or dissemination. If there is a need to collect information from the public using social media, the requestor must first work with the Office of Information (OIS) Services to obtain the appropriate OMB clearances (see MD 3.54, "NRC Collections of Information and Reports Management"). Requests may be emailed to INFOCOLLECTS.Resource@nrc.gov.

If the NRC collects PII through its use of a social media service, the agency should collect only the minimum information necessary to accomplish a purpose required by statute, regulation, or Executive Order.

(8) The NRC will ensure that the NRC Privacy Policy, accessible from the NRC Web site, describes the NRC's use of any social media services, including the following:

– the specific purpose of the NRC's use of the third-party Web sites or applications

– how the NRC will use PII that becomes available through the use of the third-party Web sites or applications

– who at the NRC will have access to PII

– with whom PII will be shared outside the NRC

– whether and how the NRC will maintain PII, and for how long

– how the NRC will secure PII that it uses or maintains

– what other privacy risks exist and how the NRC will mitigate those risks

(9) To the extent feasible, the NRC should post a privacy notice on the social media service itself. The privacy notice should do the following:

- Explain that the Web site or application is not a Government Web site or application, that it is controlled or operated by a third party, and that the NRC's Privacy Policy does not apply to the third party.
- Indicate whether and how the NRC will maintain, use, or share PII that becomes available through the use of the third-party Web site or application.
- Explain that by using the Web site or application to communicate with the NRC, individuals may be providing nongovernment third parties access to PII.
- Direct individuals to the NRC's official Web site.
- Direct individuals to the NRC's Privacy Policy as described above.

The NRC should take all practical steps to ensure that its privacy notice is conspicuous, salient, clearly labeled, written in plain language, and prominently displayed at all locations where the public might make PII available to the NRC.

The phrase "make PII available" includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects the information. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or "associates" PII while using the social media service. Associate can include activities commonly referred to as "friending," "following," "liking," joining a "group," becoming a "fan," and comparable functions.

6 Approving Use of Social Media

All requests to enable access to new social media sites for participation as an Authorized NRC Representative and for participation on official duty should be directed to the NRC Single Point of Contact (SPOC) at http://spoc.nrc.gov/Pages/default.aspx to coordinate the necessary reviews and approvals for use with OIS, Office of General Counsel (OGC), and the Computer Security Office (CSO) as appropriate.

Proposals to establish a NRC official presence site using a social media service must be directed to OPA as indicated in section 6.1 below. NRC offices are responsible for ensuring appropriate approvals are obtained through OPA prior to use of social media sites for NRC official presence.

6.1 Office of Public Affairs Review and Approval

In assessing the creation of an official NRC-sponsored social media site or account, OPA will consider the benefit to the NRC of the most commonly used social media sites first and determine if any meet the needs of the NRC to do the following:

- Provide a wider distribution of existing content to reach members of the general public, especially those not currently using existing means to obtain NRC information.

- Allow for the distribution of newly created content that can "tell the NRC story" in new ways.

- Allow for creative dialogue, expanded outreach, and relationship-building with external audiences/stakeholders.

As part of its analysis, OPA will study how other Federal agencies and industry sources use the most common social media tools (e.g., YouTube, Twitter) so that the NRC can build on their successes and avoid issues they have encountered. OPA will also consider available resources, capabilities, limitations, content management, and other issues before deciding to create an NRC official presence on a particular social media site.

Once a site has been identified as meeting the business criteria, OPA will work with OIS, CSO, and OGC to resolve technology, information management, security, and legal issues, and establish site/accounts. OPA will announce the launching of any NRC official presence site with a press release and Network Announcement.

NRC employees may suggest social media sites to OPA for consideration for official presence sites by e-mailing opa.resource@nrc.gov. The e-mail should include information about the tool/site and how it could be used to promote NRC activities, mission, goals, positions, policies, and actions to the general public.

6.2 Office of the General Counsel Review and Approval

Once a request for social media use has been submitted, OGC will review the social media platform (e.g., YouTube,Twitter) (1) before initial implementation by an NRC office of the social media platform, (2) when an office proposes to use a social media platform's functions or services not previously evaluated by OGC, or (3) when there has been a change to associated terms of service for a social media platform. OGC's review of social media platforms proposed for use by the NRC will evaluate whether the use of a social media platform can conform to all applicable laws, regulations, and policies. The provision of no legal objection by OGC to a particular social media platform is dependent upon the ability of the office that has proposed the initial use of the social media platform to satisfy the requirements determined by OGC to be necessary to conform to the use of the social media platform to all applicable laws, regulations, and policies. OGC will maintain a list of those social media platforms for which it has provided no legal objection to use.

6.3 Information Technology Implementation/Modification Review and Approval

All new IT implementations (e.g., implementing an official NRC sponsored social media site) or modifications to existing IT implementations (e.g., enabling access to a particular social media Web site) must be reviewed and approved in accordance with NRC IT policy, procedures, and standards. NRC Privacy Impact Assessment (PIA), which is required by Project Management Methodology (PMM), assesses privacy risks, implements privacy protections, and determines record retention and disposal schedules. Applicable MDs include MD 2.6, "Information

Technology Infrastructure"; MD 2.8, "Project Management Methodology (PMM)"; MD 3.2, "Privacy Act"; MD 3.53; MD 3.54; MD 12.2; MD 12.5; and MD 12.7.

7 Links to Other NRC Policies

MD 2.6, "Information Technology Infrastructure"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md2.6.pdf

MD 2.7, "Personal Use of Information Technology"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/MD2.7.pdf

MD 2.8, "Project Management Methodology (PMM)"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md2.8.pdf

MD 3.1, "Freedom of Information Act"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md3.1.pdf

MD 3.2, "Privacy Act"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md3.2.pdf

MD 3.4, "Release of Information to the Public"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md3.4.pdf

MD 3.53, "NRC Records and Document Management Program"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md3.53.pdf

MD 3.54, "NRC Collections of Information and Reports Management"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md3.54.pdf

MD 5.5, "Public Affairs Program"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md5.5.pdf

MD 7.3, "Participation in Professional Organizations"
http://www.internal.nrc.gov/policy/directives/catalog/md7.3.pdf

MD 12.2, "NRC Classified Information Security Program"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md12.2.pdf

MD 12.5, "NRC Automated Information Security Program"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md12.5.pdf

MD 12.7, "NRC Safeguards Information Security Program"
http://www.internal.nrc.gov/ADM/DAS/cag/Management_Directives/md12.7.pdf

"NRC Agency-wide Rules of Behavior for Authorized Computer Use" (ADAMS Accession No. ML082190730)
http://www.internal.nrc.gov/CSO/documents/ROB.pdf

Sensitive Unclassified Non-Safeguards Information (SUNSI) Handling Requirements
http://www.internal.nrc.gov/sunsi/

OMB M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies"
http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf

OMB M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications"
http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.