Next Steps: Social Media for Emergency Response

Virtual Social Media Working Group and DHS First Responders Group

January 2012

Homeland Security

Science and Technology

CONTENTS

INTRODUCTION

Social media and collaborative technologies have become critical components of emergency preparedness, response, and recovery. From the international response efforts after major tsunamis to hurricane recovery in major U.S. cities, many government officials now turn to social media technologies to share information and connect with citizens during all phases of a crisis. Implementing these new technologies, however, requires that responding agencies adopt new communication strategies and engagement methods.

Recognizing the need to address these challenges, the U.S. Department of Homeland Security's Science and Technology Directorate (DHS S&T) established a Virtual Social Media Working Group (VSMWG). The mission of the VSMWG is to provide guidance and best practices to the emergency preparedness and response community on the safe and sustainable use of social media technologies before, during, and after emergencies.

Drawn from a cross-section of subject matter experts from federal, tribal, territorial, state, and local responders from across the United States, VSMWG members are establishing and collecting best practices and solutions that can be leveraged by public safety officials and responders throughout the nation's emergency response community. Below is a list of agencies to which the VSMWG members belong.

VSMWG Member Agencies as of July 2011

- American Red Cross
- Bellingham [Washington] Fire
- Boca Raton [Florida] Police
- Boynton Beach [Florida] Police
- Charlotte [North Carolina] Fire
- City of Milwaukee [Wisconsin] Police
- City of Seattle [Washington] Public Utilities
- Clark [Washington] Regional Emergency Services Agency
- Fairfax County Office of Public Affairs [Virginia]
- Federal Emergency Management Agency (FEMA) Office of External Affair
- Fort Bend County [Texas] Health and Human Services
- Johnson County [Kansas] Emergency Management Division
- Montgomery County [Maryland] Fire and Rescue
- Philadelphia [Pennsylvania] Office of Emergency Management
- Philadelphia [Pennsylvania Department of Public Health
- Portland [Oregon] National Incident Management Organization, U.S. Forest Service
- North Dakota Citizen Corps, State Community Emergency Response Team (CERT)
- Rural/Metro [EMS] of San Diego [California]
- Show Low [Arizona] Fire Department

PURPOSE

This document serves as a follow-up and supporting document to the VSMWG's **Social Media Strategy**. While the Social Media Strategy provides an introduction to social media, its benefits for public safety, and examples and best practices, this document provides considerations and detailed next steps for public safety agencies developing and implementing social media.

The VSMWG developed this document with input from the public safety community through online engagement hosted on the DHS First Responder Communities of Practice portal and through online discussions via other social media channels. It is intended for use by all public safety disciplines and all types of agencies to better understand and utilize social media and other Web-based tools without having to "reinvent the wheel" or spend hours searching for examples or policy templates or guidance. This document provides considerations and best practices for the emergency response field in the development of a social media program.

The purpose of this document is to:

- Provide guidance to public safety agencies developing social media strategies and programs;
- Discuss challenges and considerations related to social media specific for agency use; and
- Provide best practices and policy examples for inclusion in agency strategies.

Examples included in this document are not intended to serve as an all-inclusive list but rather to provide a brief listing of agencies that use social media for public safety purposes. For more information on these topics and additional resources, please visit **DHS First Responder Communities of Practice** (www.communities.firstresponder.gov).

DEVELOPING A STRATEGY

The key to developing a social media strategy is not to focus on existing tools, but on the goals, objectives, strategy, and implementation procedures necessary to support the use of social media by an organization, and how to adapt to emerging technologies and communications trends over time.

An agency's social media plan is more than just a social media policy, just as the rules of the road differ from instruction on how to drive a car. The policy details the world we live and act in; the plan details how we work within that world. For most in the emergency response field, writing a social media plan can be straightforward, especially when it is understood that the plan should reside within their current all-hazards communications plan. Simply put, adding social media to your communications plan is akin to adding another tool to the toolbox; there is no need to start from scratch.

When developing supporting policies, be sure to incorporate feedback from all applicable departments, including Information Technology (IT), Legal, Human Resources, etc. A well-conceived social media policy will help guide employees, contractors and volunteers as they utilize social media for agency purposes.

Some things to consider when developing polices include:

- **Human Resources**
  - Resources required;
  - Training and education required;
  - Job descriptions;
  - Liability; and
  - Ethical conduct and accountability to an agency's rules of conduct (personal versus professional use of social media tools and technologies).
- **Operational and Communications Security (OPSEC and COMSEC)**
  - Classification and handling guidelines (e.g., For Official Use Only, Sensitive But Unclassified, Classified, etc.);
  - Training and education;
  - Devices (e.g., personal versus agency-provided, etc.); and
  - Integration with existing tools and processes.
- **Legal and Compliance**
  - Copyright laws;
  - Records retention requirements;
  - Endorsement of products, services, and postings;
  - Public disclosure and Sunshine laws; and
  - Privacy.
- **Business Continuity**
  - Necessary access rights and password policies; and
  - Redundancies.
- **Information Technology**
  - Bandwidth and other resources (servers, etc.);
  - Training and education; and
  - Integration.
- **Communications and Engagement**
  - Messaging;
  - Metrics and measuring success; and
  - Outreach.

An ever-growing list of social media policies from both public agencies and private corporations is available online at http://socialmediagovernance.com/policies.php and at the United States Department of Homeland Security First Responder Communities of Practice "Make America Safer through Social Media" community, one of the many communities found at the First Responder Communities of Practice available at http://www.communities.firstresponder.gov. These policies may serve as a starting point from which to develop an agency's strategy and supporting documents.

CHOOSING THE RIGHT TECHNOLOGY

There are hundreds of social media tools available for use by the public safety community. To ensure the best use of technology and resources, an agency should consider assessing their goals, capabilities, and

objectives for using social media, as well as agency and/or jurisdiction-specific security and IT compliance and regulations before beginning a program.

Agencies should keep in mind that the tools that are popular today may not maintain popularity over time. Technology is dynamic and fast-paced; additionally, communications trends change rapidly, and can even change in the middle of an event. Therefore, an agency should consider the following questions when choosing the types of tools that best fit the agency's goals and objectives, resources available, audience, and intended applications while remaining flexible to adapt as technology and trends change over time.

Before choosing a technology (or multiple technologies), an agency should assess its capabilities and capacity to engage with its community. Specifically, an agency should ask the following questions:

- Does your agency have an Emergency Public Information plan in place?
- For what purposes will you use social media (communications and/or situational awareness and monitoring)?
- Will social media enhance your agency's communications plan?
- Will the agency's culture accept social media as a standard procedure?
- Do you have support from your leadership for the use of social media?
- Do elected officials understand/use social media?
- Who are the power users, both internal and external? How do they use social media?
- Are current media/communications policies restrictive toward social media tools?
- Is there an IT infrastructure to support social media? What are the agency's teleworking policies?
- Does agency staff have smartphones, etc.?

The next step is choosing the right technology. When considering the vast number of tools available, agencies should:

- Determine the intended purpose for communication and/or information gathering;
- Understand the capabilities and limitations of potential channels/medium;
- Determine the longevity and stability of the platform;
- Understand user needs and how much bandwidth/support you will need to ensure tools are maintained, even during disasters (surges in use);
- Consider proprietary vs. open-source technologies (also whether the technology charges for subscriptions or if it is free of charge);
- Consider leveraging established user group versus building tools from scratch;
- Identify and compare operational support requirements;
- Identify and compare security and IT requirements;
- Consider integration with existing platforms such as mobile, media, call centers and website;
- Incorporate flexibility within policies and procedures for technology adoption as requirements will change with technology advances over time; and
- Remember that technology can be free – support and maintenance may incur costs.

To help chose the right social media tool, please consult the decision matrix in Figure 1, below, which explains the basic limitations, messaging types, and audiences for various tools.

Figure 1: Choosing the Right Tool: Decision Matrix

Tool	Limitations	Messaging Type	Non-Comprehensive Audience List
Blogging	• Non-official Web address • Information rarely pushed out	• Long-form • May include images • Can include links to sources • Can be published in multiple languages	• Frequently more educated • Regular access to internet • Information seekers • Deaf/Hard of hearing/non-English speaking
Microblogging	• Hard ceiling on message character count • May require recipient account • Difficult to transmit in multiple languages	• Short-form • Can include links to sources/other media • Immediate/local messages	• Mobile users • Tech-savvy • Deaf/Hard of hearing
Image Sharing	• Image description can be character-limited • Context of image unknown/difficult to establish • Difficult to provide access to additional material/sources	• Images with associated commentary	• Deaf/Hard of hearing/non-English speaking
Video Sharing	• Bandwidth/storage intensive • Imposes context/point of view • Requires specialized equipment to create • Requires special accommodations for non-hearing/non-English	• Video • Long-form exploration of concepts • Interviews • Can provide a face/personality to a matter • Demonstration of physical events	• Tech-savvy • Information seekers • Frequently younger
Podcasting	• Requires special accommodations for non-hearing/non-English • Requires specialized equipment to create	• Audio • Long-form exploration of concepts • Interviews	• Mobile users • Information seekers • Frequently older • Blind

SMS Messaging	• Hard ceiling on message character count • Difficult to transmit in multiple languages • Text only • Cost of sending/receiving messages • Unfamiliarity by novice users • Opt-in only	• Short-form • Immediate/local messages	• Mobile users • Less tech-savvy • Information seekers
Social Networks	• May require membership and/or "friending," "liking", or "following" to view messages • Advertising visible on profile pages	• Status updates • Announcements • Discussion (if two-way enabled with comments)	• Community groups • Mobile users (if mobile app available for download) • Frequently younger
Location-based Networks	• Low level of uptake in general public • Requires specialized equipment • Concerns about privacy • May require recipient account	• Hyper-local messaging • Short-form • May allow images/links to more information/sources	• Tech-savvy • Frequently younger
Event-based Networks	• Low level of uptake in general public • Concerns about privacy • May require recipient account	• Allows for pre-event messaging, with hyper-focus • Short-form • May allow images/links to more information/sources • Hyper-local messaging	• Tech-savvy • Frequently younger
Document Sharing	• Low level of uptake in general public • May require recipient account	• Long-form • Multiple variations of single document in multiple languages/formats • Distribution platform	• Tech-savvy • Frequently younger

Virtual Worlds	• Requires recipient account • Bandwidth intensive • Low level of uptake in general public	• World/game dependent; may be more conducive to engagement versus direct messaging due to platform and world-specific activities and/or tasks	• Tech-savvy

ENGAGING YOUR AUDIENCE

Social media is not just a tool for emergency response, but one that can enhance traditional activities within all phases of the disaster lifecycle, from preparedness and mitigation to response and recovery. Public safety agencies must utilize social media on a regular basis in order to establish their brand as a credible and reliable source for important information, as well as to encourage familiarity with their online presence within their community and with partners. Without sporadic interaction, the community, including individuals and the media, may be less likely to seek and share information originating from an agency.

Setting Expectations with Your Community

A common concern related to social media is that of the public's expectations in using social media in place of more traditional channels, such as 911. While social media may prove useful in future 911 capabilities, neither the technology nor the resources needed to support such endeavors currently exist. Public safety agencies should set expectations with their community now; sending sporadic messages out via all communications channels reminding the public of the appropriate channels for specific types of information.

Many public safety agencies using tools like Facebook and Twitter include a disclaimer stating that they do not monitor the tool 24 hours a day, that not all posts will be viewed in a timely manner (especially during an emergency), and reminding the public to only use 911 for life- threatening information. Setting expectations early is important to ensure the public understands how to appropriately leverage agency social media.

Planning and Preparing for the Unexpected

Despite an agency's greatest efforts to interact with the community and to encourage participation and interaction from all members, the organic nature of social media and virtual information sharing, especially during an emergency, will produce unexpected results. Agencies must prepare for the unexpected, and remain flexible to respond to the flow of information as it occurs.

For example, recent disasters have illustrated a trend in ad hoc and spontaneous volunteers and groups entering the social media marketplace to fulfill specialized information needs. From solicitation and management of donations to visualization and mapping of events, categorization of perceived needs received via social media channels (e.g., tweets from those affected stating needs for shelter, and water; or providing information on road closures, flood waters, etc.), ad hoc groups now offer a means of additional support to traditional response organizations.

Agencies should monitor social media for the existence of these types of groups, if only to ensure their efforts are in the public's best interest. Agencies may consider reaching out to these groups where appropriate to establish credibility and a relationship (if these groups exist prior to an event, doing so prior to the onset of a disaster), and linking to their efforts via agency profiles and Websites. Further interaction may include the development of a mechanism by which agencies can digest the data collected by these groups to better inform decision making and improve situational awareness within Incident Command. Another mechanism to develop would be one that could delegate responsibility to these ad hoc groups for donation and volunteer management.

Community Engagement

"Social Media are obviously about more than how we reach out to the public and educate the public…It's about the public talking to us. It's also about the public talking to the public."

– Nathan Huebner, U.S. Centers for Disease Control and Prevention

By assessing your community, choosing the right tools, crafting appropriate messaging, and encouraging interaction and participation, agencies can successfully leverage social media to enhance traditional means of community outreach and engagement. To begin development of a social media program, agencies are encouraged to consider the following actions.

Assess Your Community

- Assess your community's current expectations for civic engagement.
- Assess how the public expects to communicate with response officials.
- Assess the community's utilization of social media tools.

Choose the Right Tools

- Monitor how other agencies are using social media tools.
    - Pay close attention to popular community tools like blogs, bulletin boards, etc. and how the public is using these tools.
- Answer the following questions about the target audience.
    - Who are you trying to reach with social media and what tools do they use?
    - What are the best tools and methods for reaching vulnerable populations?
- What are the limits of the tools you are using to disseminate information? [See **Choosing the Right Tool Decision Matrix** (Figure 1) for more information.]

Craft Appropriate Messaging

- Who in your agency is responsible for crafting your messages?
    - Pay close attention to work burden when defining responsibilities.
    - What is the approval process for social media messages?
    - How much messaging should be creating and pre-approved in anticipation of need to disseminate in emergency situations?
- What is the continuity plan for the event that one individual is not able to release information?
- Does the agency's messaging need to adhere to interoperability regulations and/or will it need to standardize messaging for dissemination via several channels?

- Strongly encourage messaging that adheres to best practices in accessibility for all recipients.
- Craft messaging based on evidence-based audience segments.

Encourage Interaction and Participation

- Is the agency willing to allow two-way communications (comments, questions, etc.) on your social media profiles?
- If someone replies to, comments on, or otherwise acts on your social media message, do you have an obligation to respond or acknowledge that message?
- Consider developing or adapting a flowchart or decision matrix to assist in comment approval and/or deletion. The United States Air Force comment approval flowchart is one such resource.[1]

Two-way communications may enhance community engagement for several reasons. First, it empowers individuals to provide information to each other and provides a forum in which to share and request information between the public and an agency. Two-way communications may also encourage feedback from the community regarding response efforts. For example, community members may cite specific needs not yet known to a response agency. However, if an agency engages in two-way communications, agency social media profiles will need to be monitored during emergencies to ensure that such valuable messages are forwarded to the appropriate unit.

CHALLENGES AND BEST PRACTICES

Use of social media can be fraught with missteps and anxiety if expectations are not set with the public and employees from the beginning. Social media practitioners, by and large, advocate the theory of "failing fast." To "fail fast" means to try something—anything—and if it doesn't work, try something else. This means it's best to start using social media today before the emergency.

There are no hard-and-fast rules for how best to use social media. What works for one agency or campaign may not work for another. Below is a list of potential concerns and recommended practices to mitigate those concerns. Please note: this list is not meant to be exhaustive, but rather a sampling of common concerns and best practices for overcoming them. Challenges and concerns may change as technology advances.

Privacy

- Disclosing the use of "cookies" for information retention and "data mining;"
- Setting the privacy settings so the public can view information posted on social media profiles (versus just profile "Friends"); and
- Discouraging users from disclosing personal information (e.g., phone numbers, addresses, date of birth, etc.) by publishing reminders periodically.

Content-Based Restrictions (Comment Policies)

Content should not be restricted unless restriction is narrowly tailored to achieve compelling government

[1] http://www.globalnerdy.com/wordpress/wp-content/uploads/2008/12/air_force_web_posting_response_assessment-v2-1_5_09.pdf

interest or public quality. Such conditions meriting restriction include the promotion of discrimination, promotion of political campaigns, encouragement of illegal activity, compromised public safety or security, legal ownership issues, or solicitation of commerce. Additional examples include:

- Not prohibiting content that criticizes officials or disagrees with agency postings, articles, or proposed policies or regulations. Do monitor for appropriateness, posting monitoring procedures and "rules of behavior," and encourage the community to report misuse.
- Limiting the use of social media tools that disable posting of comments.
- Considering protected health information and monitor to ensure it is not shared via profiles.
- Many federal agencies have posted their comment policies online at www.Facebook.com/government. Consider using these as a starting point for crafting your own agency-specific policies.

Public Disclosure Laws

Communication between two officials via any format or system including social media is considered to meet the threshold for public disclosure laws in most areas. Some things to consider include:

- Ensuringing training and education programs/policies are in place within the agency to encourage safe use of social media by government officials.
- Considering posting information regarding public disclosure laws on social media profiles.
- Recognizing that technology cannot be used to eliminate the need for physical meetings.

Records Retention

- All posted content including that of "friends" or "followers" must be subject to the same retention laws.
- Make social media content available in offline formats for people who lack access.
- Ensure all profiles are in compliance with Section 508 regulations.

Health Information

Examine the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule closely. It is enforced by the Office of Civil Rights and prohibits the release of health information that can be linked to and/or identify a person. Entities required to comply with HIPAA privacy laws may oppose use of social media for this reason alone.

Agencies required to follow this federal law include any agency participating in Emergency Medical Services as a community responder, first responder or transport responder, as well as other government programs (See Health and Human Services' "For Covered Entities"). These types of agencies may have an extremely strict mindset about releasing information of any kind; including a lawyer in their decision to participate in social media platforms may be helpful.

To counteract concerns regarding release of information protected by HIPAA, consider:

- Developing training for users of social media with regards to information covered by HIPAA.
- Posting messages on social media profiles alerting users to types of information covered by HIPAA

and therefore not to be shared via social media.
- Including restrictions in any posted rules of behavior, frequently asked questions, etc.
- Monitoring social media profiles for release of HIPAA-protected information.

Human Resources

Social media may require additional or specific skills – consider including characteristics in future job descriptions to ensure appropriate hiring. Additional points to consider include:

- Conducting a brief assessment of existing personnel and skill sets, leveraging existing resources and expertise where possible.
- Considering Fair Labor Standards Act (FLSA) restrictions; specifically, would the inclusion of social media in an employee's responsibilities require an exemption if the employee must work after hours to update social media during surge or disaster events?

Information Technology (IT)

Consider existing IT guidelines or restrictions with which your agency must comply and how the addition of social media technologies might affect compliance. Many agencies maintain legacy anti-blogging policies. However, most agencies have not yet revised these polices to include micro-blogging, such as Twitter. Additional points to consider include:

- Identifying guidelines for employees representing an agency or larger jurisdiction. Are those using social media on behalf of the agency aware of IT guidelines?
- Considering IT-related contracts and who is able to enter into contracts with third-party providers on behalf of the agency. Often, social media sites require members to "check a box" signifying acceptance of the third-party rules of behavior or service agreements. This action may equate to entering into a contract on behalf of the agency.
- Consulting with your agency's legal department often to ensure they are aware of your actions and understand your goals, objectives, and purpose for using social media.
- Considering social media tools offering corporate or enterprise use (e.g., Google Maps, etc.). Individuals using tools under corporate licenses may not have authority to do so.

Security

Challenges associated with the security of social media technology are often artificial. Social media tools are open in nature and encourage participation. An employee's use of social media technology via open networks is no more of a threat than visiting other Websites, if the employee has been educated on the rules of "safe surfing." Most often user error is what leads to security breaches, not the technology itself.

Information of concern typically resides on classified networks, which has standards that will often mitigate concerns related to security breaches and social media. If you are not dealing with sensitive information, you are likely working within an open network, and therefore are no more susceptible to security breaches by allowing social media use than not. Additional points to consider include:

- To understand security concerns, defining "Security" as related to social media. For example:
    - What type of information are you trying to share, and at what handling level?

    - With whom are you sharing information?
    - Who else may have access to shared data via social media channels, and does your agency have a concern about sharing data with other individuals?
- For classified environments, considering dedicating a user-specific computer for access to social media technologies.
- Including the following topics in security training to inform employees of potential vulnerabilities and risks to using the internet in general and social media specifically, including:
    - Personally Identifiable Information and how not to release it (and the implications of releasing data in aggregate);
    - Common safety procedures (e.g., not opening suspicious e-mails, not sharing passwords, etc.);
    - Privacy (and lack thereof if using social media on behalf of an agency); and
    - Password operational security procedures (OPSEC);

If an employee states they work for a specific agency within their profile, they may need to comply with agency rules of ethics. Remind employees that any information shared via a profile in which they have identified themselves as an employee of an agency may be subject to review by that agency for legal or human resources matters.

In addition to training, establish OPSEC and Communications Security (COMSEC) protocols dictating employee behavior on social media technologies. These may include:

- Ensuring employees are familiar with "safe surfing" etiquette (for both personal and professional reasons) as well as with agency protocols for security breaches.
- Ensuring employees understand the capabilities of social media tools and the implications of changing account settings, and update them often. Many social media sites change privacy and account setting features on a regular basis.
- Understanding types of social media profile settings and what profile types are appropriate for agency use (e.g., the difference between types of profiles on a social networking site). Different types of profiles offer different features, including what type of information is shared with whom.
- Keeping an open mind and remaining flexible. Technology advances quickly – developing a sustainable process and protocol may help frame standards and future IT-related decisions.
- Considering what infrastructure you may need for future decisions (e.g., additional network connections, laptops, etc. at an emergency operations center, etc.).
- When applicable, considering continuity of operations requirements, including redundant servers, password sharing, delegation of authority, and other standard continuity practices.

NEXT STEPS

There are several steps to adopting new technologies and methodologies, each of which require careful consideration and planning. These include the following:

- Choosing the right technology and applications;
- Strategy, policy, and procedure development;
- Setting and managing expectations;
- Engaging the community;
- Managing misinformation; and
- Addressing challenges to adoption, including concerns related to privacy, public comment, record retention, public disclosure, health information, human resources, information technology, and security.

Following publication of this document, the Virtual Social Media Working Group will continue to serve as leaders within the field of public safety on the safe and sustainable use of social media. The group will continue to collect, analyze, and aggregate information, considerations, lessons learned, and best practices.

For more information about the DHS Virtual Social Media Working Group and to participate in discussions regarding the use of social media for public safety, please visit DHS First Responder Communities of Practice at www.communities.firstresponder.gov.