Department of Homeland Security

Office of Inspector General

New Media for Offices of Inspectors General: A Discussion of Legal, Privacy and Information Security Issues

This report was prepared on behalf of Council of the Inspectors General on Integrity and Efficiency

OIG-13-121

September 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

September 16, 2013

Preface

At the request of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Homeland Security Roundtable (HSR) and with the approval of the CIGIE Executive Council, the Department of Homeland Security (DHS) Office of Inspector General (OIG) chaired the New Media Working Group (Working Group), consisting of public affairs specialists, attorneys, information technology (IT) professionals, and other subject matter experts, to assess OIG use of new media.

In September 2011, the Working Group produced *Recommended Practices for Offices of Inspectors General Use of New Media*. The report discusses current and prospective uses of new media tools in the OIG community and suggests practices that OIGs may use as they consider implementing such tools. CIGIE endorsed the recommendations in the report, including establishing a permanent standing working group on emerging technologies and their impact on the OIG community, and issuing an educational guide on legal, privacy, and information security new media issues.

This report implements one of the recommendations to CIGIE. It is a product of permanent standing working group attorneys and information security specialists from 13 OIGs. We trust that this report will guide OIGs as they use or consider using new media to further the OIG mission. We express our appreciation to all who contributed to the preparation of this report.

Charles K. Edwards
Deputy Inspector General

Table of Contents

Appendixes

Abbreviations

apps	applications
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
DHS	Department of Homeland Security
DLP	data loss prevention
EO	Executive Order
FACA	*Federal Advisory Committee Act*
FAQ	frequently asked questions
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	*Federal Information Security Management Act of 2002*
FOIA	*Freedom of Information Act*
Fed. Reg.	*Federal Register*
FTCA	*Federal Tort Claims Act*
GAO	U.S. Government Accountability Office
GSA	General Services Administration
HR	human resources
IG	Inspector General
IP	Internet protocol
IT	information technology
LEP	Limited English Proficiency
MSPB	Merit Systems Protection Board
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OGE	Office of Government Ethics
OIG	Office of Inspector General
OLC	Office of Legal Counsel

OMB	Office of Management and Budget
PCIE	President's Council on Integrity and Efficiency
PIA	Privacy Impact Assessment
PII	personally identifiable information
PRA	*Paperwork Reduction Act*
SaaS	Software as a Service
SAOP	Senior Agency Office for Privacy
SORN	Systems of Record Notice
SP	Special Publication
Title VII	Title VII of the *Civil Rights Act of 1964*
TOS	terms of service

Council of the INSPECTORS GENERAL on INTEGRITY and EFFICIENCY

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) was statutorily established as an independent entity within the executive branch by the *Inspector General Reform Act of 2008*, Public Law 110-409. The mission of the CIGIE is to—

- Address integrity, economy, and effectiveness issues that transcend individual government agencies; and

- Increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the Federal Office of Inspector General (OIG) community.

Membership

- All Inspectors General (IGs) whose offices are established under either section 2 or section 8G of the *Inspector General Act*, or pursuant to other statutory authority (e.g., the Special IGs for Iraq Reconstruction, Afghanistan Reconstruction, and Troubled Asset Relief Program)

- The IG of the Intelligence Community and the Central Intelligence Agency

- The IGs of the Government Printing Office, the Library of Congress, the Capitol Police, the Government Accountability Office, and the Architect of the Capitol

- The Controller of the Office of Federal Financial Management

- A senior-level official of the Federal Bureau of Investigation, designated by the Director of the Federal Bureau of Investigation

- The Director of the Office of Government Ethics

- The Special Counsel of the Office of Special Counsel

- The Deputy Director of the Office of Personnel Management

- The Deputy Director for Management of the Office of Management and Budget (OMB)

CIGIE Homeland Security Roundtable

Since September 11, 2001, protecting our Nation has been a paramount concern of the entire Federal establishment. The OIG community plays a significant role in reviewing the performance of agency programs and operations that affect homeland security. To a large extent, this has been accomplished through collaborative efforts among multiple OIGs.

On June 7, 2005, the President's Council on Integrity and Efficiency (PCIE) Vice-Chair established a PCIE Homeland Security Roundtable. The roundtable supports the OIG community by sharing information, identifying best practices, and participating on an ad hoc basis with various external organizations and government entities. The CIGIE New Media Working Group was formed under the auspices of the Homeland Security Roundtable.

Executive Summary

The rapid expansion and growing popularity of new media, including interactive social media, is creating both opportunities and challenges for Federal Inspectors General. This report, produced by the Council of Inspectors General on Integrity and Efficiency (CIGIE) New Media Working Group, is designed to give detailed guidance to Inspectors General and their staffs on legal, privacy, and information security issues related to the use of social media.

This report follows up on the New Media Working Group's initial effort published in September 2011. *Recommended Practices for Offices of Inspectors General Use of New Media* presented Inspector General views on new media based on a survey sent to 79 CIGIE members, generally analyzed issues involving OIGs and emerging technologies, and made six recommendations to OIGs and one recommendation to CIGIE.

This report focuses on two Office of Inspector General (OIG) uses of new media: official use, such as for public affairs outreach and human resources purposes, and unofficial use by employees. It does not cover OIG uses of new media in the law enforcement, national security, or intelligence contexts, and its guidance may not apply equally in those contexts. The report provides guidance on a range of legal and policy issues, including constitutional considerations, information and privacy, accessibility, ethics, terms of service, intellectual property, information collection, liability, and records management. It also offers insights into the information security challenges inherent in installing, hosting, monitoring, and managing official new media ventures. Although the Working Group has strived to draft a reader-friendly report, written for lay people as well as specialists, the issues that this report presents cover a wide variety of apparently disparate topics and concerns. The variety of topics reflects the breadth of experience and knowledge that OIGs must employ to address new media issues.

Our research and analysis is intended to help not only the larger offices that may already have a new media program or are starting one, but also the smaller offices with fewer resources. Regardless of whether an OIG already uses, is planning to use, or is not intending to use social media, policies and safeguards should be developed since many, if not most, employees are already individually engaged in this new cyber community.

This report should not be used as a substitute for independent legal advice.[1] This is a fluid area, and laws and policies may change at a rapid pace.

This report makes no recommendations.

[1] The CIGIE New Media Working Group members and sponsors expressly disclaim liability for errors and omissions in the contents of this report. No warranty of any kind, implied, expressed, or statutory, is given with respect to the contents. The information appearing in this report is for general informational purposes only and is not intended to provide legal, privacy, or information security-related advice to any individual or entity. We urge you to consult with your own legal, privacy, or information security advisor before taking any action based on information appearing in this report.

Background

As discussed in the 2011 Council of Inspectors General on Integrity and Efficiency (CIGIE) report, new media encompasses all forms of electronic, digitized, and interactive media, including tools that allow users to share content through text, images, audio, and/or video. New media applications (apps) may be hosted internally or obtained through cloud services. New media tools such as SharePoint and the Office of Management and Budget (OMB) MAX platform facilitate knowledge management, collaboration, and internal communication within the Federal Government, whether intra-agency or government-wide.

This report covers such tools to an extent but focuses to a great degree on social media, a subset of new media that allows for public interaction, collaboration, and participation. Types of social media include collaborative projects (e.g., Wikipedia, wikis), blogs and microblogs (e.g., Twitter), media sharing websites (e.g., YouTube, Flickr), social or professional networking websites (e.g., Facebook, MySpace, LinkedIn, Google+), and virtual social worlds (e.g., Second Life).

The legal, privacy, and information security framework will vary depending on where the new media is hosted, such as whether it is hosted internally by an OIG, or externally, such as Software as a Service (SaaS) or third-party websites and apps. In addition, the analysis may change depending on whether the new media is used to share internally or externally, and whether the external information sharing is unidirectional, coming solely from an OIG, or allows input and sharing from the public.

Legal and Privacy Considerations

Regulating Speech Under the First Amendment

Like other employers, OIGs have an interest in monitoring employee performance and conduct, and not just while employees are at work. Increasingly, employees' professional lives and personal lives are merged, with employees broadcasting via social media networks their views about their work, coworkers, and supervisors. Employers, including government employers, may not always like what employees have to say. Yet while private sector employers may extend their workplace policies to the online and virtual world without considering First Amendment implications, a government employer must balance the need to regulate speech with employees' First Amendment rights.[2] In the new media environment, these obligations constitute a highly nuanced and ever-changing area of law.

[2] The First Amendment states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.

In addition to balancing employee rights with employer needs, OIG decision makers need to consider the First Amendment when regulating speech on official new media websites: specifically, whether allowing or disallowing public commentary on an OIG-sponsored new media website will affect any First Amendment analysis. Intentionally allowing the public to participate and comment on an official social media website raises First Amendment issues if the OIG wants to edit or restrict any of the commentary. It is wise to consider the purpose of the social media website, or "public forum," ahead of time since an OIG's intent and purpose for a social media website will largely determine the standard the courts use to evaluate whether an OIG appropriately and legally regulates comments.

The following discussion of First Amendment implications in relation to new media includes an overview of the public forum doctrine; official government usage or the "government speech" doctrine; regulating public and internal platforms; unofficial, non-work-related employee use of new media; and First Amendment guidance in a social media policy.

Overview of the Public Forum Doctrine

The Supreme Court employs "forum analysis" to determine when the government may limit or exclude expressive activity in public property or places where people assemble or debate.[3] Traditionally, the Supreme Court evaluated speech restrictions on the government's physical or "tangible" property, such as an amphitheater, but the Court expanded the analysis to include non-traditional "property," such as a university meeting facility or school board meeting.[4] Although applying forum analysis to such a "metaphysical" or virtual world as new media is relatively new, it can be done.[5]

[3] Christian Legal Soc'y Chapter of the Univ. of Cal., Hastings Coll. of the Law v. Martinez, 130 S. Ct. 2971, 2984 (2010).
[4] *See* Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983) (citing Widmar v. Vincent, 454 U.S. 263 (1981) (university meeting facilities); City of Madison Joint School District v. Wisconsin Employment Relations Comm'n, 429 U.S. 167 (1976) (school board meeting); Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546 (1975) (municipal theater)).
[5] OIGs may not own the digital spaces in which they use new media but can still create public forums in those areas. A forum does not even need to exist spatially or geographically; it may be metaphysical. *See Christian Legal Soc'y*, 130 S. Ct. at 2979 (public forum precedents supply the appropriate framework for the speech and association rights claims regarding student-group funding and school email lists at a public law school); Rosenberger v. Rector and Visitors of Univ. of Va., 515 U.S. 819, 827 (1995) (funding for student activity publications constitutes a public forum). *Cf.* David S. Ardia, *Government Speech and Online Forums: First Amendment Limitations on Moderating Public Discourse on Government Websites*, 2010 BYU L. REV. 1981, 1993 (2010) ("It remains an open question whether these virtual spaces will inherit the same protections for speech that we take for granted in the physical world.").

Generally, under the "public forum doctrine," government official use of new media may fit into one of three forum categories[6]: "designated" public forum, "limited" public forum (which may be considered a subcategory of a designated public forum), or "nonpublic" forum. The lines between these categories are not always clear.[7]

Courts have found that the government creates a designated public forum when government property that has not traditionally been regarded as a public forum is "intentionally opened up for that purpose."[8] Examples include a public university auditorium or municipal theater.[9] New media platforms likely constitute designated public forums when they are interactive and allow the public to express themselves, particularly if it is the agency policy or practice to create such a forum.[10] Having such a policy or practice indicates intent to designate areas "for expressive activity by citizens."[11] The Supreme Court has made intent the key determinant of whether a forum is public or nonpublic.[12] When the government regulates speech in designated public forums, courts will evaluate the government's regulations under "strict scrutiny," meaning that the "restriction must be narrowly tailored to serve a compelling government interest," and restrictions based on viewpoint are prohibited.[13]

A limited public forum is a subset of a designated public forum, where the government may limit access to certain groups or topics, as long as the restrictions are reasonable and viewpoint-neutral.[14] When the government excludes a speaker based on the subject matter of his speech, the exclusion need only be reasonable and viewpoint-neutral.[15] When the government excludes a speaker who falls within the class to which a designated public forum is made generally available, however, or excludes a speaker

[6] A fourth "traditional public forum" category includes areas such as streets or parks that "have immemorially been held in trust for the use of the public." *Perry*, 460 U.S. at 45 (quoting Hague v. Comm. for Indus. Org., 307 U.S. 496, 515 (1939)). Since the government has not held new media sites open historically or immemorially for public speech, it is unlikely that a court would find that the government created a traditional public forum with external new media tools, so we will not further analyze this category. *See* Ardia, *supra* note 5, at 1998 ("Given the Internet's short history, there is little chance that a website, or indeed anything on the Internet, would be considered a traditional public forum").

[7] Lyrissa Lidsky, *Government Sponsored Social Media and the Public Forum Doctrine Under the First Amendment: Perils and Pitfalls*, 19 THE PUB. LAWYER 2 (Summer 2011).

[8] Pleasant Grove City, Utah v. Summum, 555 U.S. 460, 469 (2009). To determine whether the government intended to create a limited public forum, courts look to the government's "stated purpose" and "objective indicia of intent," such as "the *consistent* policy and practice of the government." Bryant v. Gates, 532 F.3d 888, 896 (D.C. Cir. 2008) (emphasis in original) (quoting Stewart v. Dist. of Columbia Armory Bd., 863 F.2d 1013, 1016-17 (D.C. Cir. 1988)).

[9] *Perry*, 460 U.S. at 45.

[10] *Id*. at 47.

[11] Lyrissa Lidsky, *Public Forum 2.0*, 91 B.U. L. REV. 1975, 1998 (2011); *see also* Ardia, *supra* note 5, at 1998-99 ("In the end, it is likely that a government website that allows private speech will be viewed under the public forum doctrine as a limited public forum – that is, 'public property which the state has opened for use by the public as a place for expressive activity.'") (quoting *Perry*, 460 U.S. at 45)).

[12] *E.g.*, Cornelius v. NAACP Legal Def. & Educ. Fund, 473 U.S. 788, 802-03 (1985).

[13] *Summum*, 555 U.S. at 461.

[14] *Perry*, 460 U.S. at 46; Christian Legal Soc'y Chapter of the Univ. of Cal., Hastings Coll. of the Law v. Martinez, 130 S. Ct. 2971, 2984 (2010).

[15] *Summum*, 555 U.S. at 470.

whose speech obviously falls within the subject matter constraints of the forum, the government's action is not judged by whether it is reasonable and viewpoint-neutral but is subject to strict scrutiny.[16] In other words, if an OIG opened a forum for congressional staffers to discuss open OIG recommendations, excluding a staffer discussing that topic must be judged under strict scrutiny, but excluding him because he is not discussing open OIG recommendations needs only to be reasonable and viewpoint-neutral.

Finally, a nonpublic forum is "[p]ublic property that is not by tradition or designation a forum for public communication."[17] Government internal use, such as SharePoint or an internal wiki or blog, would fall under this category. The government may make "time, place, and manner" restrictions on speech in this forum, and may regulate to "reserve the forum for its intended purposes, communicative or otherwise, as long as the regulation on speech is reasonable and not an effort to suppress expression merely because public officials oppose the speaker's view."[18] Courts examine only the reasonableness of government regulations because the government has not "dedicated" this property to speech activity.[19]

Official Government Speech

Public forum analysis does not apply to the government speech doctrine because, as the name implies, this is when the government speaks for itself.[20] First Amendment free speech protections do not apply when the government expresses its own views.[21] For example, tweets from an official government account are not subject to First Amendment protections because the government is tweeting its own message. When an OIG uses a social media website solely to share information about its programs and related issues but allows no public commentary or participation, the government speech doctrine would apply.[22]

This option is the easiest to manage in that it raises no First Amendment issues, yet it may not allow an OIG to take full advantage of social media. Most people would argue that allowing public participation is the point of social media; it is not meant to be a one-way street. Decision makers should consider their goals before setting up a social media account, and if they see no benefit of engaging the public, then settling for this option should be fine. Whatever an OIG decides, it is important to avoid using the

[16] Ark. Educ. Television Comm'n v. Forbes, 523 U.S. 666, 677 (1998); *see also Cornelius,* 473 U.S. at 802.
[17] *Perry*, 460 U.S. at 46.
[18] *Id*.
[19] *Id.*
[20] *Summum*, 555 U.S. at 464.
[21] *Id*. at 467-68.
[22] Lidsky, *supra* note 11, at 1996 ("A non-interactive Facebook page controlled by a government actor would doubtless be treated as government speech. . . .").

government speech doctrine as a pretext for regulating private speech on government property, such as a public forum.[23] See Table 1, First Amendment Categories.

Table 1: First Amendment Categories

Type	Example	Regulation Standard
Designated Public Forum	• Interactive new media that allows public comments • Determining factor is intent	• Strict scrutiny • Restrictions based on viewpoint prohibited
Limited Public Forum	• New media that may allow public interaction but restricts access to certain groups, topics, or individuals	• Restrictions must be reasonable and viewpoint-neutral • If government excludes speaker whose speech falls within subject matter constraints of forum, however, subject to strict scrutiny
Nonpublic Forum	• Internal new media, such as SharePoint or an internal wiki or blog	• Time, manner, place restrictions acceptable • Must be reasonable • Can reserve forum for intended purposes
Government Speech	• Official OIG social media that pushes out message unidirectionally • No public participation	• The First Amendment does not apply

Regulating Public Platforms

At times it may be unclear whether an OIG is speaking for itself or has created a public forum. In most cases involving new media there will be a mixture of government and private speech.[24] For example, when an OIG engages the public through its blog or Facebook page, it likely creates a limited public forum in the comments section of each "post."[25] In those cases, the OIG should regulate public speech according to the limited or designated public forum context, as appropriate.

Under the public forum doctrine, OIGs may not discriminate against speech solely because of the viewpoint expressed. Only when the regulation is reasonable and necessary to preserve the purpose of the forum may an OIG regulate who may speak in new media limited public forums and what is said in those forums. For example, when an OIG blogs about its most recent audit report, it may delete comments to the post that are off-topic or entirely unrelated to the audit or OIG programs, but it would be improper to delete comments that express displeasure with the results or opinions of an OIG audit. Additionally, OIGs may remove comments that advertise nongovernmental products, services, or organizations because such speech may be an improper

[23] *See Summum*, 555 U.S. at 473 (acknowledging the "legitimate concern that the government speech doctrine not be used as a subterfuge for favoring certain private speakers over others based on viewpoint").
[24] Lidsky, *supra* note 11, at 1997-98.
[25] *Id*. at 1999 ("There is little doubt that [interactive social media] sites are forums, at least with regard to the comments portion of the site.").

endorsement under Federal ethics rules.[26] Finally, OIGs will want to remove any information resulting from public participation that may identify a specific person, such as a Social Security number, photograph, or date of birth. Participants need to be advised that they should not post such information.

OIGs also may encounter issues with indecent or vulgar commentary on external new media websites. OIG account managers may restrict or remove "unprotected speech"[27] from new media websites so long as they do not narrowly apply the unprotected speech rules to discriminate against certain views.[28] Unprotected speech includes fighting words,[29] words that imminently incite illegal behavior,[30] threats,[31] and obscenities or obscene material.[32]

Additionally, speech on new media websites that does not rise to the level of unprotected speech under the First Amendment may still disrupt the purpose of the forum and thus may call for removal. Several courts have upheld restrictions on speech in public meetings to maintain decorum and limit discussion to the purpose of the forum, as long as they do not discriminate based on a speaker's viewpoint.[33] Accordingly, an OIG may adopt a policy prohibiting personal attacks or disruptive speech, as long as the policy is content-neutral and is intended to maintain decorum in the forum.[34]

However, it is important to recognize that unlike in-person meetings, new media users can more easily disregard personal attacks or repetitive, off-topic comments by skimming through comments or ignoring comments altogether. Given how easy it is to ignore speech on new media platforms, OIGs should consider whether removing certain

[26] *See infra* Ethics section.
[27] The Supreme Court has stated that certain types of speech are not entitled to protection because they are "of such slight social value . . . that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality." Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).
[28] *See* R.A.V. v. City of St. Paul, Minn., 505 U.S. 377, 388 (1992) (providing the example that a state might "choose to prohibit only that obscenity which is the most patently offensive in its prurience" but may not prohibit only obscenity that includes offensive political messages.).
[29] *Id*. at 383; Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942) ("[T]he lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words'—those which by their very utterance inflict injury or tend to incite an immediate breach of the peace"—do not enjoy constitutional protection).
[30] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).
[31] Watts v. United States, 394 U.S. 705, 707 (1969).
[32] Miller v. California, 413 U.S. 15, 24 (1973) (indicating that obscene material as that which appeals only to prurient, or sexually arousing, interests; depicts "patently offensive" sexual conduct; and lacks any "serious literary, artistic, political, or scientific value").
[33] *E.g.*, Steinburg v. Chesterfield Cnty. Planning Comm'n, 527 F.3d 377, 385 (4th Cir. 2008) (a planning commission meeting was a limited public forum, and the city could limit its discussion and restrict speakers reasonably to preserve decorum necessary to accomplish the purpose of the meeting).
[34] *Steinburg*, 527 F.3d at 387 ("A content-neutral policy against personal attacks is not facially unconstitutional insofar as it is adopted and employed to serve the legitimate public interest in a limited forum of decorum and order").

borderline off-color comments, for the purpose of upholding decorum and reasonably preserving the purpose of the forum, is worth the risk of chilling free expression.[35] While remaining mindful of obligations regarding privacy, OIGs should consider disallowing anonymous speech. Requiring users to register before posting comments might encourage appropriate use of the forum and, as long as the information is accessible to users who do not wish to register with a third-party provider, is advisable.[36] However, OIGs should not require users to provide their personal information to a third-party provider to access government content. Not only could this raise privacy issues, but also it may create the appearance of providing preferential treatment to an enterprise.[37]

Regulating Internal Platforms

An OIG may create a new media platform solely for internal purposes, such as to allow employees to communicate with each other or share a digitized collaboration space. Unless the public is allowed to access the website and participate, the forum would be a nonpublic forum. An OIG may restrict internal new media access to a specific subset of employees in a nonpublic forum. For example, an OIG may grant access on a case-by-case basis, as in a SharePoint website for auditors or when a need-to-know basis exists. An OIG could even open an internal website to selected nongovernmental groups, potentially creating a limited public forum. The "constitutional right of access" would extend only to other entities of the same character, however; the Supreme Court has held that "selective access," or allowing only certain similar groups to join a forum, does not transform a limited or designated public forum into a public forum.[38]

OIGs have much more freedom to regulate speech in nonpublic, internal forums, as these forums are only subject to the reasonableness and viewpoint-neutral limitations. These limitations would not be violated if, for example, OIGs were to delete off-topic posts in SharePoint discussions or deny certain employees access to forums because of a lack of need-to-know. Despite employee requests for anonymity, OIGs may require employees to identify themselves before posting to internal new media platforms to ensure accountability.

[35] *See* Lidsky, *supra* note 11, at 2002, for arguments as to why "allowing the government to preserve decorum in public meetings do not apply as strongly in the social media context."
[36] *See infra* Information and Privacy, and Public Accessibility sections for more information.
[37] 48 C.F.R. § 301-1 requires government business to be conducted "with complete impartiality and with preferential treatment for none." *See also infra* Information and Privacy section regarding third-party privacy policy issues.
[38] Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 47 (1983).

Unofficial Employee Use of New Media

Regarding unofficial employee use of new media, Federal employees do not forfeit their First Amendment rights by virtue of their employment.[39] However, the Supreme Court has recognized that the government "may impose restraints on the job-related speech of public employees that would be plainly unconstitutional if applied to the public at large."[40]

Absent proof of false statements knowingly or recklessly made, a public employee has the right to comment as a citizen on matters of public concern.[41] However, when a public employee speaks not as a citizen upon matters of public concern, but instead as an employee about personal matters, government officials may take disciplinary action for inappropriate behavior or speech. As the Supreme Court has held, "[w]hen employee expression cannot be fairly considered as relating to any matter of political, social, or other concern to the community, government officials should enjoy wide latitude in managing their offices, without intrusive oversight by the judiciary in the name of the First Amendment."[42] For example, "private speech" involving a complaint about changes to an employee's duties may give rise to discipline,[43] as may other speech that does not meet the public concern threshold, such as employees' speech made "pursuant to their official duties."[44] Examples of official-duty speech include job-related or media interviews, or anything that may fall within an employee's duties. Absent unusual circumstances, a Federal court will not second-guess an OIG personnel decision based on private speech, even if it is unfair or unreasonable.[45]

[39] Federal courts of appeals have held that the government may not condition employment based on waiving a constitutional right. *See* Pickering v. Bd. of Educ., 391 U.S. 563, 568 (1968) (teachers do not lose their First Amendment rights to comment as citizens on matters of public interest in connection with the schools where they work); Keyishian v. Bd. of Regents, 385 U.S. 589, 605-06 (1967) ("The theory that public employment, which may be denied altogether may be subjected to any conditions, regardless of how unreasonable, has been uniformly rejected.").

[40] United States v. National Treasury Employees Union, 513 U.S. 454, 465 (1995).

[41] *Pickering*, 391 U.S. at 571-73 (high school teacher wrongfully dismissed for openly criticizing the Board of Education on its allocation of school funds between athletics and education, and its methods of informing taxpayers about the need for additional revenue because they were "matter[s] of legitimate public concern" upon which "free and open debate [was] vital to informed decisionmaking by the electorate"). *See* Garcetti v. Cabellas, 547 U.S. 410 (2006); Connick v. Myers, 461 U.S. 138 (1983).

[42] *Connick*, 461 U.S. at 146.

[43] *Nat'l Treasury Employees Union*, 513 U.S. at 466.

[44] *Garcetti*, 547 U.S. at 421 ("When public employees make statements pursuant to their official duties, the employees are not speaking as citizens for First Amendment purposes, and the Constitution does not insulate their communications from employer discipline.").

[45] *Connick*, 461 U.S. at 146-47 ("Ordinary dismissals from government service which violate no fixed tenure or applicable statute or regulation are not subject to judicial review even if the reasons for the dismissal are alleged to be mistaken or unreasonable.").

First Amendment Guidance in a Social Media Policy

Social media users, including Members of Congress and judges, sometimes fail to realize that information on social networks can be disseminated more widely and used for purposes other than intended. OIG employees are no exception. Experience has shown that absent a policy, the boundaries between social media use and office functions can become blurred. For example, law enforcement officers have posted material that has impeached their courtroom testimony, or caused them to be removed from Federal service, and inappropriate social media use could easily harm an audit.[46] Employees need to know that their private social media use may be discoverable, and not everything is protected by the First Amendment.[47]

Policies on employee use of social media are essential to help prevent employee missteps and protect the agency. All policies should have one baseline: Employees must make sure that their personal use of social media never creates conflicts with the work of their agency or OIG. All employees are responsible for ensuring that no information is disclosed through social media that might compromise OIG investigations, audits, or inspections. An OIG policy might contain the following language:

- Expressing personal views pursuant to one's official duties, whether on or off duty, may result in disciplinary action.[48]

- Employees not authorized to speak on behalf of OIG must avoid giving the impression that they are representing OIG's views.[49] Therefore, when appropriate, employees should be clear that they are speaking solely in their personal capacity and not representing the OIG.

- Whether authorized to speak for OIG or not, employees may be disciplined for certain types of speech. Statements generally not afforded First Amendment

[46] *See* J. Dwyer, *The Officer Who Posted Too Much on MySpace*, N.Y. TIMES (Mar. 10, 2009), http://www.nytimes.com/2009/03/11/nyregion/11about.html. Dwyer interviewed an officer whose MySpace posts allowed someone to beat a felony weapons charge at State Supreme Court, Brooklyn. The arresting officer posted before the trial that he was feeling "devious" and was "watching [violent police movie] to brush up on proper police procedure." *See also* Spivey v. Dep't of the Navy, 2012 MSPB LEXIS 5278 (MSPB 2012) (police officer removed from services for posting sensitive law enforcement information on Facebook).

[47] *E.g.*, Trail v. Lesko, No. GD-10-017249 (C.P. Pa. July 3, 2012) (before a requesting party will be granted unfettered "access" to a Facebook account, the party must show a "sufficient likelihood" that the nonpublic postings would contain information that is relevant to the litigation that is "not otherwise available"). The *Lesko* analysis varies from the standard threshold relevancy model adopted by some courts and uses a balancing approach based on the "level of intrusiveness." This opinion is an introduction to the discoverability of private social media content in Pennsylvania and other jurisdictions.

[48] *Garcetti*, 547 U.S. at 421.

[49] Under 5 C.F.R. § 2635.702(b), government employees are prohibited from creating the appearance that the government sanctions their views or activities. In addition, 5 C.F.R. § 2635.807(b)(2) requires employees involved in teaching, speaking, or writing, to provide a disclaimer that the views expressed do not express the views of the U.S. Government.

protection include those that reflect solely matters of internal or personal interest; false and defamatory statements about OIG and/or OIG employees; threats and insults; "fighting words;"[50] and statements that unduly disrupt the office, undermine a supervisor's authority, or destroy necessary close working relationships.[51]

- Generally, employees may express themselves as private citizens about matters of concern and value to the public at large,[52] unless such speech undermines OIG's effectiveness and efficiency.

- The First Amendment does not prohibit managerial discipline based on an employee's speech made pursuant to official responsibilities because, in such a case, the employee speaks as an employee and not as a private citizen.[53] The First Amendment protects only speech that an employee makes as a private citizen concerning a matter of public concern.

While a policy should be clear, it should not be too proscriptive. For example, a policy should not state that employees must allow OIG to vet blog posts before publication or require employees to get permission before posting a video on YouTube. Unless they are "reasonably necessary to protect the efficiency of the public service,"[54] such restrictions are likely to be seen as a prior restraint on free speech and struck down by a court.[55]

[50] Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942) ("[T]he lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words'—those which by their very utterance inflict injury or tend to incite an immediate breach of the peace"—do not enjoy constitutional protection). *See also* R. A. V. v. St. Paul, 505 U.S. 377, 383 (1992) (categories of expression can, consistently with the First Amendment, be regulated "*because of their constitutionally proscribable content* (obscenity, defamation, etc.)" (emphasis in original)).

[51] *E.g.*, Rankin v. McPherson, 483 U.S. 378, 388 (1987) (*Pickering* balance test considers such government interests in efficient office functioning as "whether the statement impairs discipline by superiors or harmony among coworkers, has a detrimental impact on close working relationships for which personal loyalty and confidence are necessary, or impedes the performance of the speaker's duties or interferes with the regular operation of the enterprise"); City of San Diego v. John Roe, 543 U.S. 77, 84 (2004) (upholding city's termination of police officer whose off-duty conduct brought the mission of the city police department and the professionalism of its officers into serious disrepute, and whose speech was not a matter of public concern).

[52] *E.g.*, Pickering v. Bd. of Educ., 391 U.S. 563, 574 (1968) ("[A]bsent proof of false statements knowingly or recklessly made," a public employee's speech on matters of public concern may not form the basis of dismissal).

[53] Garcetti v. Cabellas, 547 U.S. 410, 421 (2006).

[54] United States v. National Treasury Employees Union, 513 U.S. 454, 474 (1995).

[55] *E.g.*, Harman v. City of New York, 140 F.3d 111, 119 (2d Cir. 1998) (agency policy requiring prepublication review of any information an employee intended to convey to the media was a prior restraint because it attempted to suppress speech in advance rather than punish disruptive remarks after their effect was felt); Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, 559 (U.S. 1975) ("a free society prefers to punish the few who abuse rights of speech after they break the law than to throttle them and all others beforehand"); Cf. Weaver v. United States Info. Agency, 87 F.3d 1429, 1436 (D.C. Cir. 1996) (regulation permissible because the need to protect against the dissemination of sensitive material outweighed employee's rights, but if it were read to authorize punishment or suppression of speech in advance, it would "raise serious constitutional issues").

The Fourth Amendment and the Expectation of Privacy

Another constitutional consideration of new media concerns the Fourth Amendment.[56] Government activity implicates the Fourth Amendment when government personnel conduct a "search" or a "seizure." The Fourth Amendment protects citizens from unreasonable government intrusions into areas that are "constitutionally protected"[57] or where an individual has a reasonable expectation of privacy.[58] Depending on the policies and practices at an OIG, protected areas may include new media (and specifically, social media) activity on OIG-issued electronic devices and computers. No court that we know of has found new media to be a "constitutionally protected area" for Fourth Amendment purposes.[59] Therefore, individuals will enjoy Fourth Amendment protection in their use of new media only when they have a reasonable expectation of privacy, which requires an "actual, subjective expectation of privacy" that society is prepared to recognize as "objectively reasonable."[60]

There can be no reasonable expectation of privacy in social media activities that do not restrict access, such as social media posts without privacy settings, because users knowingly expose their activities to the public.[61] Accordingly, members of the public, and Federal employees who post information on social media accounts that are accessible to the public, have no reasonable expectation of privacy in those posts. For example, if a member of the public posts on an official OIG government social media account, he or she does not have a reasonable expectation of privacy in that information. Similarly, if a Federal employee tweets a message on her personal Twitter account but allows her account to be visible to the public, she has no reasonable expectation of privacy in her tweets. In addition, users may not expect privacy in noncontent, routing information of their Internet connections, such as to/from

[56] The Fourth Amendment states that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause. . . ." U.S. CONST. amend. IV.
[57] Jones v. United States, 132 S. Ct. 945, 951 (2012) (government's warrantless installation of a GPS tracking device on a personal vehicle constituted a search because it was a trespass upon a constitutionally protected effect, *i.e.*, a vehicle, for the purpose of obtaining information). Constitutionally protected areas include individual's persons, houses, papers, and effects. U.S. CONST. amend. IV.
[58] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[59] *But see* EDWARD C. LIU, ET AL., CONG. RESEARCH SERV., R42409, CYBERSECURITY: SELECTED LEGAL ISSUES 19, n. 145 (2012) (suggesting a court could find email to be a "paper" and a packet of data to be an "effect" under the Fourth Amendment).
[60] *Katz*, 389 U.S. at 361.
[61] *Id.* at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (a person "has no legitimate expectation of privacy in information he voluntarily turns over to third parties"). Social media users also have no reasonable expectation that information they voluntarily provide to others, such as other social media users in their networks, will remain private. *See* United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D. N.Y. 2012) (a Facebook user's "legitimate expectation of privacy ended when he disseminated posts to his 'friends' because those 'friends' were free to use the information however they wanted").

addresses for emails, Internet Protocol (IP) address of websites visits, volume of use, and other addressing and routing information.[62]

Federal employees do not lose Fourth Amendment protections by virtue of their Federal employment.[63] The government may not require employees to waive their Fourth Amendment rights as a condition of employment,[64] such as by requiring an employee to provide passwords to his or her personal social media accounts. Nor may the government require an employee to provide unfettered access to an employee's personal computer or handheld devices, such as an iPhone or Blackberry.[65]

While a government employee may have a reasonable expectation of privacy in the workplace, however, a government employer may take steps to reduce or eliminate that expectation.[66] Employees using their government computers for personal use to communicate with friends via social media, for example, may have a subjective belief that their posts are private. Whether such expectation is objectively reasonable, and therefore entitled to Fourth Amendment protection, depends on the facts and circumstances of each situation.[67]

Even when an employee has a reasonable expectation of privacy in the workplace, an OIG may conduct a warrantless search without violating the Fourth Amendment under the "special needs" exception,[68] or as long as it is not excessive in scope and is reasonably related to a work purpose.[69] An employer's "special needs" for efficient and proper operation of the workplace make the probable cause and warrant requirements impracticable and unnecessary for legitimate, reasonable, work-related, noninvestigatory intrusions, and investigations of work-related misconduct.[70] To

[62] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008). *See also* Smith, 442 U.S. at 743-44 (no legitimate expectation of privacy in dialing, routing, addressing, and signaling information transmitted to telephone companies).
[63] *See* O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (plurality opinion).
[64] Federal courts of appeals have held that the government may not condition employment based on waiving a constitutional right. *See, e.g.*, McDonnell v. Hunter, 809 F.2d 1302, 1310 (8th Cir. 1987) (if a search is unreasonable, "a government employer cannot require that its employees consent to that search as a condition of employment"); Keyishian v. Bd. of Regents, 385 U.S. 589, 605-06 (1967) ("The theory that public employment, which may be denied altogether may be subjected to any conditions, regardless of how unreasonable, has been uniformly rejected.").
[65] *See infra* Human Resources section for additional analysis on employee relations.
[66] Whether an employee has a reasonable expectation of privacy in the workplace depends on several factors, including (1) the openness and accessibility of the workspace, (2) whether the employee has exclusive use of an area or item, (3) if the employer gave the employee prior notice of the possibility of searches in that area, and (4) the employer's common practice and procedure of searching the area. Thompson v. Johnson County Cmty. Coll., 930 F. Supp. 501, 507 (D. Kan. 1996) (factor 1); United States v. Taketa, 923 F.2d 665, 673 (9th Cir. 1991) (factor 2); Schowengerdt v. United States, 944 F.2d 483, 488 (9th Cir. 1991) (factor 3); Am. Postal Workers Union v. United States Postal Serv., 871 F.2d 556, 560-61 (6th Cir. 1989) (factor 3); *O'Connor*, 480 U.S. at 717-18 (factor 4).
[67] *O'Connor*, 480 U.S. at 717 (noting that the determination of whether a government employee has a reasonable expectation of privacy in the workplace requires a case-by-case analysis).
[68] *Id*. at 725.
[69] *O'Connor*, 480 U.S. at 725; City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010).
[70] *Id*.

determine whether the special needs warrant exception applies, the Court balances an employee's privacy expectations with the government's interests.[71]

Reducing or Eliminating Employees' Privacy Expectations

Although the Supreme Court has not addressed the issue, Federal courts have held that agencies may reduce or eliminate government employees' expectation of privacy when using government computers or devices through regulations and agency practices, such as policies, consent banners, and computer-user agreements.[72] For example, the Fourth Circuit held that an employee did not have a legitimate expectation of privacy regarding his Internet use at work because his agency's policy advised that the employer would electronically audit and monitor users' access.[73] Therefore, the OIG warrantless search of the employee's computer and removal of his hard drive from his office did not violate the Fourth Amendment.[74]

Accordingly, OIGs should develop and implement a policy that notifies employees that they have no legitimate expectation of privacy whenever they are using a government-issued electronic device or computer, and similarly, that data exchanged on government equipment may be used by the government for official purposes. OIGs also should require employees to consent to an appropriately worded log-on banner and computer-user agreement.

[71] Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665 (1989). If the government's needs trumps an employee's privacy interests—and as long as a Federal employer has a legitimate, work-related reason to intrude on an employee's privacy expectations, and the intrusion is "reasonable under the circumstances"—the government does not need a warrant to conduct a search. *Id*. "Dual purpose" situations, in which the employer conducts a reasonable search based on a legitimate, work-related need, and also finds evidence of criminal conduct, do not require a warrant. The government does not lose its "special need for the efficient and proper operation of the workplace" merely because the evidence obtained revealed a crime. *O'Connor*, U.S. 480 at 723.

[72] *E.g.,* United States v. Thorn, 375 F.3d 679, 683 (8th Cir. 2004), *cert. granted, judgment vacated on other grounds,* 543 U.S. 1112 (2005), *judgment reinstated*, 413 F.3d 820 (8th Cir. 2005) (policy eliminated state employee's reasonable expectation of privacy in the contents of the computer); United States v. Angevine, 281 F.3d 1130, 1134-35 (10th Cir. 2002) (banner and computer policy eliminates a state university professor's reasonable expectation of privacy in data downloaded from the Internet); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (Air Force sergeant had no reasonable expectation of privacy in his government email account because it was reserved for official business and network banner informed him that use was subject to monitoring); United States v. Hamilton, 778 F. Supp. 2d 651, 654 (E.D. Va. 2011) (computer use policy defeated public school employee's expectation of privacy when computer use policy stated that contents of the computer were subject to inspection, defendant signed forms acknowledging the policy, and a banner informed him of this policy when logging on to the system); Wasson v. Sonoma Cnty. Junior Coll. Dist., 4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997) (public employer's computer policy giving the employer the right to access all information stored on the employer's computers eliminates an employee's reasonable expectation of privacy in files stored on the computers); Bohach v. City of Reno, 932 F. Supp. 1232, 1235 (D. Nev. 1996) (police officers do not retain a reasonable expectation of privacy in their use of a pager system because of order announcing that all messages would be logged).

[73] United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).

[74] *Id*.

To ensure compliance with the Fourth Amendment and other laws implicating Fourth Amendment concerns, the Department of Justice's Office of Legal Counsel (OLC) recommends the following model log-on banner language:[75]

- *You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.*
- *Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.*
- *By using this information system, you understand and consent to the following:*
  - *You have no reasonable expectation of privacy regarding communications or data transiting or stored on this information system.*
  - *At any time, and for any lawful government purpose, the Government may monitor, intercept, and search any communication or data transiting or stored on this information system.*
  - *Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.*

[click button: I AGREE]

If an OIG decides to implement its own banner language and computer-user agreements, care should be given to ensure that any diminution of an employee's expectation of privacy is explicit and comprehensive. No matter how explicit a banner is, though, the Federal Law Enforcement Training Center's *Legal Division Handbook* warns agencies against relying on them exclusively, so it is advisable to consult counsel before conducting an electronic search.[76]

Information and Privacy

In addition to constitutional issues, OIGs must consider information and privacy issues for both outbound and inbound communications when implementing a social media program. Three key information and privacy laws come into play in the new media context: the *Privacy Act of 1974*, as amended (*Privacy Act*);[77] the *E-Government Act of 2002*, as amended (*E-Government Act*);[78] and the *Freedom of Information Act* (FOIA), as amended.[79] An OIG needs to ensure not only its own compliance with these three laws,

[75] Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. 1 2009, 5-6 (2009) [hereinafter Legal Issues Relating to EINSTEIN 2.0].
[76] U.S. DEP'T OF HOMELAND SEC., FEDERAL LAW ENFORCEMENT TRAINING CENTER LEGAL DIVISION HANDBOOK 434 (2012).
[77] 5 U.S.C. § 552a.
[78] Pub. L. No. 107-347, 116 Stat. 2899 (codified as amended at scattered sections 44 U.S.C.).
[79] 5 U.S.C. § 552.

but also compliance of any third-party social media provider whose products it uses. Generally, each social media provider has its own privacy policy. An OIG should direct the public to read each third-party policy carefully before participating or providing information.

The *Privacy Act of 1974*

The *Privacy Act* is the primary law governing how the Federal Government collects, uses, maintains, and disseminates information about individuals. It protects records about individuals when such records are maintained in a "system of records" under the agency's control[80] and are retrieved from that system by name, Social Security number, or any other identifier assigned to the individual.[81]

With certain exceptions, the *Privacy Act* prohibits disclosure of such records to any person or other agency without the written consent of the individual(s) to whom the records pertain.[82] In addition to the exceptions that are contained in the *Privacy Act*, additional exceptions appear as "routine uses" in a "System of Record Notice" (SORN) published in the *Federal Register*. Any OIG implementing a social media program should review the exceptions and ensure that all *outbound* social media communications that contain *Privacy Act*-protected information comply with one of the exceptions.[83]

The *Privacy Act* also generally requires that agencies provide individuals the right to access, amend, and correct their records,[84] although OIGs have traditionally exempted their investigatory files under the *Privacy Act* from this requirement.[85] Regarding

[80] The *Privacy Act* also applies to government contractor-operated systems of records. 5 U.S.C. § 552a(m).
[81] *Id*. at (a)(4), (5). Personally Identifiable Information (PII), which is generally protected by the *Privacy Act*, includes any other "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual." Joshua B. Bolten, *M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OFF. MGMT. & BUDGET (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda_m03-22 [hereinafter OMB M-03-22] (citing definition of PII from Clay Johnson III, *M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, OFF. MGMT. & BUDGET (May 22, 2007), *available at* http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf). Whether information can be used to uncover an individual's identity is determined through a case-by-case assessment of the specific risk of identification.
[82] 5 U.S.C. § 552a(b). The *Privacy Act* contains certain explicit exceptions, including internal use on a need-to-know basis, disclosures required under the FOIA, disclosures in response to certain court orders, as well as official requests of congressional committees for matters their official jurisdiction and the U.S. Government Accountability Office (GAO). *Id*. One exception allows agencies to establish additional "routine uses" (disclosures) compatible with the purpose for which the record was collected, provided those "routine uses" are published in the *Federal Register* notice establishing the relevant system(s) of records from which the records will be disclosed. *Id*. at (b)(3).
[83] *Privacy Best Practices for Social Media*, CIO Council, at 10 (July 2013), #5, *available at* https://cio.gov/wp-content/uploads/downloads/2013/07/Privacy-Best-Practices-for-Social-Media.pdf (suggesting additional requirements for sharing information collected via social media) [hereinafter CIO Council Privacy Best Practices].
[84] *Id*. at (d).
[85] *See, e.g.*, *id*. at (j)(2) (criminal investigatory files); (k)(2) (law enforcement investigatory files other than those covered by the (j)(2) exemption); and (k)(5) (investigatory materials for determining suitability, eligibility, qualification for Federal civilian

records that are not exempt, OIGs should give careful consideration to *inbound* social media communications and how (or whether) they will be treated, kept, stored, and maintained. Indeed, retaining such communications may require the creation of a new system of records, as (to use one example) comments to a blog post from the public might not fall under the definition of any existing system.[86]

Since the *Privacy Act* generally requires agencies to maintain information in their systems of records only such information about individuals that is "relevant and necessary" to accomplish an agency purpose required by statute or Executive Order (EO), it may be that much of the inbound social media communication that an OIG receives should not be maintained at all.[87] For example, while fraud allegations submitted through social media likely are "relevant and necessary," and thus may merit retention and storage, responses to tweets about an OIG initiative may not qualify.

When creating social or other new media accounts, databases, or programs, OIGs must examine whether they may be establishing a new system of records within the meaning of the *Privacy Act*. The definition of a system of records, as noted earlier, includes whether the records will be under agency "control," whether those records will be "about" individuals, and whether records will be "retrieved" from the system by name or other personal identifier.[88] If the OIG determines that it will be creating a new system of records—rather than simply incorporating records into an existing OIG system—the OIG must first seek public comment by publishing a SORN, and must also notify Congress and OMB of the proposed system.[89] This procedural requirement is not merely ministerial, as agency officers and employees can be held criminally liable if they willfully maintain a system of records without publishing the legally required SORN beforehand.[90] OIGs also may be subject to civil liability for maintaining inaccurate, out-of-date, or incomplete data collected about individuals in the OIG's systems of records, if that information is then used unfairly to make an adverse determination relating to an individual's qualifications, character, rights, opportunities, or benefits to which the individual may be entitled.[91]

---

employment, military service, Federal contracts, or classified information access, but only to the extent such material would reveal a confidential source). An agency must issue formal, published regulations in order to invoke these exemptions.

[86] For example, the Special Inspector General for Afghanistan Reconstruction has created SIGAR-11, Social Media Records, and SIGAR-12, Internal Electronic Collaboration Tools. See 77 FR 46551 (Aug. 3, 2012).

[87] 5 U.S.C. § 552a(e)(1).

[88] OIGs should consult with counsel in making this determination.

[89] 5 U.S.C. §§ 552a(e)(4), (11); *OMB Circular No. A-130, Management of Federal Information Resources*, *Revised*, OFF. MGMT. & BUDGET App. I, para. 4 (2000), *available at* http://www.whitehouse.gov/omb/circulars_a130_a130trans4 (Federal agency reporting requirements to OMB and Congress). Agencies should also make their SORNs available on their agency websites.

[90] 5 U.S.C. § 552a(i)(2).

[91] *Id*. at (e)(5), (g)(1)(C).

In light of these provisions, OIGs must carefully consider and weigh the benefits and risks of collecting, maintaining, or using Internet rumor, hearsay, and other third-party statements that may be difficult to verify. Information that an individual has directly posted on his or her own behalf may not be intended to be strictly factual or accurate, even if it may reflect the individual's personal views or state of mind at the time. As noted above, because individuals may have no legal right under the *Privacy Act* to obtain mandatory access to their investigatory files, OIGs that decide to collect such information should also consider how individuals will be able to evaluate and ensure its accuracy and reliability.[92] For example, the OIG may consider whether it is feasible or appropriate to offer an individual the opportunity to review, explain, or challenge the accuracy of such information, if it will be used as a basis for decisions regarding his or her employment, referral for prosecution, or other actions regarding the individual's rights, benefits, or privileges.

When using social media or other means (e.g., online forms and questionnaires) to collect information from individuals for any new or existing system of records, OIGs generally must include a statement, on the form used to collect the information or on a separate form that can be retained by the individual, about the OIG's authority to solicit the information, the purpose for which the information is intended to be used, routine uses, and any consequences of not providing the requested information ("*Privacy Act* statement").[93] As a result, creating a new system of records for *inbound* social media communications, or storing such communications in existing systems, creates a notice requirement in the operation of a social media program.

It should be noted that the *Privacy Act* does not prohibit agencies from maintaining records of fighting words, words that imminently incite illegal behavior, threats, and obscenities, or other such statements that may be posted on an OIG blog or online forum, so *inbound* communication of this nature can be retained and provided to appropriate authorities. But without a legitimate law enforcement purpose, consent, or statutory authority, the *Privacy Act* forbids the government from maintaining records describing how an individual exercises his or her right First Amendment rights (e.g., speech, religion, assembly), unless certain exceptions apply.[94] Therefore, collecting and

[92] For OIG investigatory files exempted solely under (k)(2), individuals have a right of access (except to information revealing a confidential source) if the individual has been denied rights, benefits or privileges on the basis of such records. *See id*. at (k)(2).
[93] *Id*. at (e)(3).
[94] 5 U.S.C. § 552a(e)(7). This restriction applies even if the agency does not maintain or intend to maintain the information in a "system of records" as defined by the Act. For a collection of cases, *see* OFFICE OF INFO. & PRIVACY, U.S. DEP'T OF JUSTICE, GUIDE TO THE FREEDOM OF INFORMATION ACT 46-47 (2009), *available at* http://www.justice.gov/oip/foia_guide09.htm [hereinafter FOIA Guide]. Note that this restriction does not require or authorize an agency to destroy any records that it has been required or authorized to collect and retain under Federal law (e.g., the *Federal Records Act*), as outlined in the Records Management section *infra*.

storing a series of tweets or blog posts for official purposes—even if relevant to the OIG's mission—may violate the *Privacy Act*.[95]

The *Privacy Act* also limits the extent to which an agency may disclose information from its systems of records about individuals without their consent. Since one of the primary OIG uses of new media is to disseminate or share information about its audit and investigative work, it is critical that such disclosures (whether in tweets, posts, or blogs) not violate the *Privacy Act*. When nonpublic information is to be communicated through new media about, for example, an OIG investigation, steps should be taken to protect the identity of the subject or others. This may require editing or redacting written documents, editing or blurring video content, or taking other steps to protect individuals' identities.

Each OIG's routine uses, already published as part of the SORN in the *Federal Register*, will guide OIG in its disclosures, but OIGs using new media may wish to revisit and, if appropriate, revise their routine uses and systems of records accordingly.[96]

The *E-Government Act of 2002* and Privacy Impact Assessments

New media fits within the 11 stated purposes of the *E-Government Act*, which include promoting citizen participation in government; interagency collaboration in providing government services; and transparency and accountability within the Federal Government.[97] OIGs must balance their pursuit of the *E-Government's Acts* goals, however, against the privacy provisions contained in Section 208 of the *E-Government Act*, designed to ensure sufficient protections for the privacy of personal information as agencies engage citizens electronically. Section 208 establishes requirements for

[95] Under Section 552a(e)(7), agencies may maintain records of First Amendment activity if "expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." Nonetheless, some agencies are finding ways to monitor social media content in compliance with the *Privacy Act*. For example, according to a Department of Homeland Security (DHS) SORN titled DHS/OPS-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records, 76 *Fed. Reg.* 5603 (Feb. 1, 2011), DHS is engaged in social media monitoring that is "not designed" to collect PII but may collect it for "certain narrowly tailored categories" and may share the information in a situation involving life and death. In June 2012, the Navy issued a solicitation that may help develop metrics tools for the public sector, allowing it to monitor the conversation "surrounding" the Navy. *See Solicitation No. N00189-12-T-Z131, Social Media Monitoring*, DEP'T OF THE NAVY (2012), *available at* https://www.neco.navy.mil/upload/N00189/N0018912TZ13112TZ131.doc.

[96] To cite some examples of agencies that have amended their system of records to account for social media, the Consumer Financial Protection Bureau has amended two of its systems of records to allow for disclosure to viewers of its social media and blog posts. See 77 FR 64962 (Oct. 24, 2012) and 77 FR 59386 (Sept. 27, 2012). The Federal Housing Finance Agency has amended a system of records to account for individuals or organizations that provide information through social media, among other methods. See 77 FR 47641 (Aug. 9, 2012).

[97] 44 U.S.C. § 3501 note. Pub. L. No. 107-347, 116 Stat. 2899, is codified as amended at scattered sections 44 U.S.C.

conducting, reviewing, and publishing Privacy Impact Assessments (PIAs), and for posting privacy policies on Federal agency websites.[98]

Government agencies are required to conduct PIAs for information technology (IT) systems (e.g., software, hardware, Web development, cloud services) that will collect, maintain or disseminate personally identifiable information (PII).[99] This assessment must take place before an agency develops in-house or procures from outside sources such IT, or before it initiates a new online collection of information within the meaning of the *Paperwork Reduction Act* (PRA), as amended, using such technology (e.g., new online web form or public survey that collects PII).[100]

As explained in OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, a PIA evaluates and documents not only how the agency will secure the PII, but also other nonsecurity issues potentially affecting privacy, including the availability or adoption of any alternative processes or technologies to mitigate such risks, and compliance with any other applicable legal, regulatory, and policy requirements.[101] These additional privacy issues in the PIA include, for example, the purpose and scope of the PII to be collected, maintained, or disseminated by the technology; how the PII will be used or shared; how the agency will provide individuals with notice and applicable consent or access rights, if any; how and when PII will be retained or destroyed; and whether a system of records will be created under the *Privacy Act*.

In addition, agencies are required to perform PIAs and update them as necessary where a system change creates new privacy risks. This may occur—

- When converting paper-based records to electronic systems;
- When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public; or
- When OIGs work together on shared functions involving significant new uses or exchanges of information in identifiable form.[102]

[98] *Id.* The *E-Government Act* also includes FISMA. For a discussion of the FISMA requirements, *see infra* Information Security section.
[99] *Id.* The *E-Government Act* uses the term information in "identifiable form," which means "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."
[100] The PRA is codified at 44 U.S.C. §§3501-20; see also 5 C.F.R. Part 1320. In general, the PRA applies when an agency poses a set of identical questions to collect information from 10 or more persons (excluding agencies, instrumentalities, or Federal employees). 44 U.S.C. § 3501, et. seq. *See infra* Information Collection section.
[101] OMB M-03-22, *supra* note 81.
[102] *Id*. Attachment A.

A PIA is not required when information relates to internal government operations or has been previously assessed under an evaluation similar to a PIA. In addition, a PIA is not required where privacy issues are unchanged, such as when government-run websites, IT systems, or collections of information do not collect or maintain information in identifiable form about members of the general public, or when there are minor changes to a system or collection that do not create new privacy risks.

Adapted PIAs and Third-Party Websites or Apps

OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, modified OMB Memorandum M-03-22's PIA guidance because Federal agency use of third-party websites and apps raised "new questions."[103] Specifically, M-10-23 requires an "adapted PIA" when an agency's use of a third-party website or app may make PII available to the agency.[104] Common examples include opening a social media account, embedding a third-party app on an official government website, or retaining a third-party developer to create and distribute an app for public use. M-10-23 sets forth the information that an adapted PIA must contain, including:

- The specific purpose of an agency's use of the third-party website or application;
- Any PII that is likely to become available to the agency through such use;
- Intended or expected use of the PII;
- With whom it will share PII;
- Whether, how, and for how long it will maintain the PII; and
- How it will secure the PII it uses or maintains.

In addition, each use of a third-party website or app should be covered in a single, separate PIA. However, a single PIA may cover multiple websites or apps if they are "functionally comparable" and the agency practices "substantially similar across each website and application."[105]

Adapted PIAs should be tailored to address specific functions of a website or app but need not be more elaborate than the OIG's other PIAs. OMB guidance emphasizes that, regardless of the third-party website or app involved, agencies must limit the collection of PII through the website or app to the minimum necessary to accomplish a purpose required by statute, regulation or EO. OIGs must also examine the third party's own

[103] *See* Peter R. Orszag, *M-10-23, Guidance for Agency Use of Third-Party Websites and Applications*, OFF. MGMT. & BUDGET (June 25, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.
[104] The term "make PII available" includes any agency action that causes PII to become available or "accessible" to the agency, whether or not the agency actually solicits that PII, or collects and incorporates it into agency records. *See id*. (defining "make available").
[105] *Id*.

privacy policy and practices carefully to evaluate the privacy risks and determine if the website or app is appropriate for OIG use.

OMB Memorandum M-10-23 also imposes specific public disclosure requirements before an agency can use a third-party website or app. First, a PIA must be posted publicly (e.g., on an OIG's official website with other PIAs), although portions that would compromise IT security may be redacted. Second, a description of the usage of the third-party website or app must be added to the agency's "privacy policy" on its website(s).[106] Third, when feasible, a "privacy notice" must be posted on the third-party website or app itself in locations where PII could be made available to the agency (e.g., an OIG social media profile or account).[107] Fourth, the agency should apply "appropriate branding" to its third-party page or app to help the public distinguish the agency's activities from nongovernment actors. In addition, M-10-23 provides that the agency's Senior Agency Office for Privacy (SAOP) be consulted in evaluating whether to use a third-party website or app, including how many PIAs are required, as the SAOP has a "central-policy making role" and "overall responsibility and accountability" for ensuring privacy protection.[108]

One final matter to consider when an OIG uses a third-party website or app is that the public must be able to obtain comparable information and services from the OIG through alternative sources.[109] In other words, the third-party website or app cannot be the exclusive means for disseminating the information or soliciting or accepting feedback. Thus, members of the public must be able to learn about an OIG's activities or communicate with an OIG in other ways, such as through the OIG's own website. Information about these alternative sources should be disclosed, for example, by linking back to the OIG's home page in the agency's privacy notice on the third-party website or app, as required by OMB's Memorandum M-10-23 and discussed earlier.

While the *E-Government Act* applies only to the government, an OIG needs to consider what social media providers do with information that the public provides in connection with OIG-sponsored activities. For example, some social media providers may try to collect PII from consumers communicating with the government in order to market to them. Some might try to collect consumer information, including photographs and

[106] *Id*. (describing what a Federal agency's privacy policy must contain, including, "when feasible," links to the relevant privacy policies of the third-party site or app).
[107] *Id.* The Privacy Notice is separate from the PIA, and discloses somewhat different information, including that the third-party site or app is not a Government site or app, and that the individual may be providing information to nongovernmental third parties. The Privacy Notice must also link to the agency's official website and Privacy Policy. An agency "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 agency" on the third-party site or app.
[108] *Id*. (citing Clay Johnson III, M-05-08, *Designation of Senior Agency Officials for Privacy* OFF. MGMT. & BUDGET (Feb. 11, 2005), available at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-08.pdf).
[109] 29 U.S.C. § 794d.

videos, to sell to businesses without notifying or paying the creators of the information. To ensure that consumers know that a third-party privacy policy governs whenever they are on a third-party website, an OIG should consider using an "about us" feature on all its social media accounts. "About us" should explain the relationship between the social media service and the OIG, and clarify which privacy policy applies and when. An OIG also should consider using a "goodbye" banner that pops up when a user leaves the OIG website. This banner should feature the privacy policy of the third-party social media website as users click to the next screen. Since users may also access OIG-sponsored social media websites directly, and not through the OIG website, an OIG should make sure that those OIG-sponsored sites contain clear language about the privacy policy that applies.[110]

Web Measurement and Customization Technologies or "Cookies"

One particularly pertinent consideration with respect to third-party websites (as well as OIG websites) is the use of "cookies," which are "small bits of software that are placed on a web user's hard drive . . . [that] can track the activities of users over time and across different websites."[111] Consistent with the *E-Government Act* and recognizing that cookies may be useful in "improv[ing] federal services online through conducting measurement and analysis of usage or through customization of the user's experience," OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies,* clarified the circumstances and conditions under which an agency may use cookies or other tracking technologies.[112] Agencies may now use single-session web measurement and customization technologies, as well as multisession technologies with and without PII, subject to certain limitations.[113]

Except for internal agency, law enforcement, national security, or intelligence activities, an OIG may not use such cookies/tracking to—

- Track user individual-level activity on the Internet outside of the website or app from which the technology originates;

[110] *See Disclaimer of Liability or Endorsement*, OFF. OF GOV. ETHICS, http://www.oge.gov/About/Website-Policies/Disclaimer-of-Liability-or-Endorsement/ (last visited Aug. 16, 2013) ("We strongly recommend that you review the policies of any outside websites you visit from this site, since you will be subject to the privacy, security, and accessibility policies of those other sites, once you leave OGE.gov.") [hereinafter OGE Disclaimer of Liability].
[111] Jacob J. Lew, *M-00-13, Privacy Policies and Date Collection on Federal Websites*, OFF. MGMT. & BUDGET (June 22, 2000), *available at* http://www.whitehouse.gov/omb/memoranda_m00-13.
[112] Peter R. Orszag, *M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies*, OFF. MGMT. & BUDGET (June 25, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf [hereinafter OMB M-10-22].
[113] Single-session technologies remember a user's online interactions using an identifier that is used only within a single session or visit, is not later reused, and is deleted immediately after the session ends. Multisession technologies remember user's online interactions through multiple sessions, using a persistent identifier for each user.

- Share data obtained through such technologies with other departments or agencies, without the user's consent;
- Cross-reference, without the user's consent, any data gathered through such technologies against PII to determine individual-level online activity;
- Collect PII without the user's consent; or
- Perform any like usages so designated by OMB.[114]

OMB M-10-22 further states that agencies may not use web measurement and customization technologies if they do not allow the public to opt out, and should explain in their privacy policies why they decided to use or not use such technologies so that users can make an informed decision on whether to opt out.

While OMB M-10-22 establishes a baseline for Federal agency compliance, OIGs have added considerations. A unique feature of many OIG websites is a page to allow the public to submit allegations of potential fraud, waste, and abuse relating to Federal programs and operations. Those reporting pages often give the user the option to submit information anonymously. Some OIGs make it clear that website and email hotline complaints are expressly not given confidentiality. However, when third-party JavaScript code for web measurement and customization is embedded on a website, a record is created that tracks, at a minimum, the IP address of individuals visiting each page. Most of these tools track users' actions to a granular level that not only identifies that they visited the main website, but also stores and tracks the steps that the users took when clicking through the website.

As a result, an individual attempting to submit information anonymously regarding suspected fraud, waste, or abuse may expect anonymity, but when correlated with other data, this tracking may be able to identify the individual. For instance, IP address information can provide relatively accurate geolocation information about the user. Furthermore, if an individual is logged into a social media service or an online email service that has an information sharing agreement with the third-party website measurement service used on the fraud submission page, it is foreseeable that sufficient information can be correlated to permit the social media service, the email service, or the third-party web measurement service (or all three) to identify the complainant.

Ultimately, the use of this third-party technology in OIG web pages creates a scenario where users believe that they are anonymously submitting information but are in fact being tracked both by the third-party website measurement service and possibly also by other business entities with which the OIG has not entered a data use agreement. The information could be held by such private companies for indefinite periods of time,

[114] OMB M-10-22, *supra* note 112.

based upon their individual privacy policies, and disclosed voluntarily or even be subject to subpoena should the private entity be embroiled in litigation.

Finally, as with third-party websites and apps, an OIG must ensure that individuals who wish to avoid tracking technologies can obtain comparable information or services without such tracking, whether on the OIG's own website or on a third-party website or app used by the OIG. For example, OIGs may allow users to opt out and access the information anyway, or they may refer users to an alternate OIG home page or other website that does not contain the tracking technology.[115]

Freedom of Information Act

Another information law issue that has arisen with respect to social media is how social media will affect OIGs' responsibilities under the FOIA.[116] The FOIA provides individuals with a right, enforceable in court, to request and obtain access to Federal agency records, except to the extent that records or portions of records are protected from public disclosure by a statutory exemption or exclusion. The E-FOIA amendments of 1996 expanded the definition of "records" to include "any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format."[117]

Government information posted on OIG websites or via third-party social media websites becomes part of the public domain upon its posting. This voluntary disclosure of information outside of the OIG may compromise the ability to withhold such information in the future under the FOIA. In addition, third-party comments may be subject to the FOIA. The Office of Government Ethics (OGE) provides the following disclaimer about what it may be required to provide under FOIA:

> *OGE may be legally required, for example, by the Freedom of Information Act or a court order, to post documents generated by third parties that may contain offensive, defamatory, or misleading or otherwise inappropriate content. The OGE disclaims responsibility for the content of these documents.*[118]

Any information created on an internal social media page would be subject to the FOIA. This information is treated the same as emails, drafts, reports, and the like, which are created electronically and are subject to the FOIA. In this case, however, because the

[115] *Id*.
[116] 5 U.S.C. § 552. FOIA presents social media issues with respect to both information and privacy, and records management. *See infra* Records Management section.
[117] *Id*. at (f)(2).
[118] *See* OGE Disclaimer of Liability, *supra* note 110.

records have not been distributed to the public, statutory exemptions could still be applied to the records.

A related issue is whether an OIG may accept FOIA requests through social media outlets. The FOIA states that an agency shall make records promptly available to any person who "reasonably describes" the records sought and requests them in accordance with the agency's published FOIA regulations.[119] Depending on the applicable regulations, it may be acceptable to receive requests using new media. The request only needs to be specific enough to enable an agency employee familiar with the subject area to locate the record with a "reasonable amount of effort."[120] OIGs must be familiar with their published FOIA regulations and make a determination if requests made through social media would be accepted.

Finally, it should be noted that OIGs are not required to provide FOIA requesters with documents that are already available to the public.[121] This includes information on the OIG's website and any publicly accessible social media content.

Information Collection

In addition to the government's responsibilities under the *Privacy Act*, *E-Government Act*, and FOIA, an OIG also should be mindful of two laws that may come into play when it receives information from the public. Before collecting information from the public, an OIG needs to consider the PRA and the *Federal Advisory Committee Act* (FACA), as amended.[122]

Paperwork Reduction Act

One of the PRA's goals is to reduce information collection burdens on the public.[123] To help achieve that goal, the PRA requires an agency to receive OMB approval before collecting information in any situation where 10 or more respondents are involved and the questions are standardized in nature.[124] The process to obtain approval involves several steps, including publishing a *Federal Register* notice and preparing an information collection request package.[125]

[119] 5 U.S.C. § 552(a)(3)(A).
[120] *See* FOIA Guide, *supra* note 94.
[121] *Id*. at 55.
[122] 5 U.S.C. app. 2.
[123] 44 U.S.C.§ 3506(b)(1)(A).
[124] 44 U.S.C. § 3502(3) (defining the term "collection of information").
[125] 44 U.S.C. § 3507.

The PRA applies to the collection of information "regardless of form or format."[126] It follows that the PRA applies to the collection of information through the use of new media and web-based interactive technologies. However, there are exceptions: OMB memorandum *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act* explains circumstances in which the PRA does not apply to social media.[127] For example, an OIG's use of blogs, wikis, and other social networks, to "publish" solicitations for public comment or conduct virtual public meetings may fall under the PRA's "general solicitations" exception.[128] This exception covers facts or opinions submitted in response to general solicitations of comments from the public, published in the *Federal Register* or other publications, regardless of the form or format, provided that no person is required to supply specific information pertaining to the commenter, other than that necessary for self-identification, as a condition of an agency's full consideration of the comment.

When seeking comments, an OIG should pose open-ended questions that solicit broad, unstructured answers, and avoid asking specific questions and disseminating surveys with identical questions. For example, an OIG may allow the public the opportunity to comment on discussion topics on blogs or other social media websites but should avoid posting web polls and satisfaction surveys that ask specific questions. An OIG may engage in brainstorming activities involving social media, such as crowdsourcing, but should avoid collecting any information beyond name and email or mailing address (e.g., age, sex, race/ethnicity, employment, or citizenship status).[129] Generally, wikis will not trigger the PRA because they "merely facilitate interactions between agencies and the public."[130] In addition, wikis and other web-based collaboration tools that are limited to internal agency use are exempt from the PRA, as are interagency wikis such as OMB MAX.[131] Finally, rankings, ratings, votes, and contests to determine a winner do not implicate the PRA unless they elicit a structured response (i.e., a series of questions that entrants must answer to take part in the contest), or if an OIG collects demographic information about the entrants.[132]

[126] 44 U.S.C. § 3502(3)(A); 5 C.F.R. § 1320.3(h).
[127] Cass R. Sunstein, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*, OFF. MGMT. & BUDG. (Apr. 7, 2010), available at http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/SocialMediaGuidance_04072010.pdf [hereinafter OMB PRA Memo].
[128] 5 C.F.R. § 1320.3(h)(4).
[129] "Crowdsourcing" is "the practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community rather than from traditional employees or suppliers." MERRIAM-WEBSTER (2013).
[130] OMB PRA Memo, *supra* note 127.
[131] *Id.*
[132] *Id.*

Federal Advisory Committee Act

The FACA governs the government's use of Federal "advisory committees." A Federal advisory committee is a group established by statute, established or used by the President, or established or used by a Federal agency to obtain advice or recommendations.[133] The Federal advisory committee process should generally be used when an OIG wants to get advice or recommendations from a group of people who are not solely Federal employees and who have an expertise or perspective which can provide value to the decision making process.

Since new media may provide a venue for open meetings and an avenue for public inspection of meeting records, an OIG's new media use may trigger FACA. For example, crowdsourcing, such as that used by www.challenge.gov or www.ideascale.com, may inadvertently lead to a FACA issue. It is important to be aware of this because FACA's administrative requirements are burdensome: If FACA applies, an agency is required, among other things, to have a charter, publish notification of meetings in the *Federal Register*, and make transcripts available to the public.[134]

Unless an OIG wishes to form an advisory committee under FACA, efforts should be made to ensure that the parties participating in meetings vary, that a consensus is not sought from participants,[135] and that the function of the group does not change to the point that an OIG begins to use the group as a source of advice or recommendations.[136]

Records Management

When collecting or maintaining information created by social media, an OIG should be aware of its recordkeeping responsibilities. All Federal agencies are required by law to manage their records.[137] The *Federal Records Act of 1950* and its implementing regulations make each Federal agency responsible for determining which records need to be preserved.[138]

[133] 5 U.S.C. app. 2, § 3(2). A committee consisting solely of Federal employees is excluded from the definition.
[134] 5 U.S.C. App. 2, §§ 9-11.
[135] The intent is to obtain information or viewpoints from individual attendees as opposed to advice, opinions or recommendations from the group acting in a collective mode. The more static the group composition (i.e., the same attendees at each meeting), the more likely a FACA issue may arise.
[136] *See* GSA, *When is Federal Advisory Committee Act (FACA) Applicable?*, available at http://www.gsa.gov/portal/content/100794.
[137] 44 U.S.C. § 3301 (defining a record, in part, as "all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them.").
[138] 36 C.F.R. § 1222.22.

Whether something is a record that must be managed and preserved depends not on the form of the record, but on the content.[139] Not all electronic data will constitute a record that requires preservation, just as not all papers are records for records management purposes. National Archives and Records Administration (NARA) guidance on records management for social media provides a nonexhaustive list of questions that may help in determining a record's status:

- Is the information unique and not available anywhere else?
- Does it contain evidence of an agency's policies, business, mission, etc.?
- Is this tool being used in relation to the agency's work?
- Is use of the tool authorized by the agency?
- Is there a business need for the information?[140]

NARA guidance indicates that if the answer to any of these questions is yes, then the content is likely to be a Federal record.[141] However, content that is duplicated across multiple platforms or held elsewhere in an agency's recordkeeping system may be considered a nonrecord. For example, NARA states that reposted news items that are captured and managed elsewhere may be considered nonrecords.[142] A NARA draft bulletin issued in June 2013 states that content on social media is likely a Federal record.[143]

To manage records created through new media, NARA advises that it may be helpful to focus on three key areas: policy, records scheduling, and preservation.[144] A records management policy for new media should provide guidance on identifying what constitutes a record in a new media platform (including user-generated content) and how such records are to be captured and managed. Once an OIG has identified new media content as records, it must schedule the records or apply an existing appropriate disposition authority. In determining if an existing schedule or a new schedule is appropriate, an OIG should consider whether the new media platform provides enhanced processes, functionality, or other features, and for how long the record must be maintained. The ways in which an OIG chooses to preserve records created through the use of new media will vary based on the platform.

Some of the options that NARA suggests to capture content include (1) saving all content with associated metadata; (2) using web crawling and software to store

[139] *Guidance on Managing Records in Web 2.0/Social Media Platforms, NARA Bull. 2011-02*, NAT'L ARCHIVES AND RECORDS ADMIN. § 4 (Oct. 10, 2010) [hereinafter NARA Bull. 2011-02]. This bulletin will expire on October 31, 2013.
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] NARA Bulletin 2013-XX, *Guidance on Managing Social Media Records*, NAT'L ARCHIVES AND RECORDS ADMIN. (June 26, 2013). This draft bulletin will supersede NARA Bull. 2011-02 but has not yet been finalized.
[144] NARA Bull. 2011-02 at § 6, *supra* note 139.

content; or (3) using web capture tools to create local versions of websites and migrating content to other formats.[145] NARA's latest guidance on preserving social media records provides a detailed list of available tools and software that could help Federal agencies in capturing social media content.[146] This document also states that screenshots do not comply with NARA's transfer guidance for permanent web content records, as they only create a picture of the content and do not preserve the content's metadata and functionality.[147]

Even when records are created and maintained on a third-party platform, an OIG is still responsible for being able to identify and retrieve them. Yet an OIG's responsibility to manage its new media records can be challenging when records reside with a third party. NARA advises agencies to include a records management clause when negotiating a terms of service (TOS) agreement.[148] The TOS should underscore OIG's responsibility to manage Federal records created through the use of the new media platform. NARA provides the following general clause:

> *The Agency acknowledges that use of contractor's site and services may require management of Federal records. Agency and user-generated content may meet the definition of Federal records as determined by the agency. If the contractor holds Federal records, the agency and contractor must manage Federal records in accordance with all applicable records management laws and regulations, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), and regulations of the National Archives and Records Administration (NARA) at 36 CFR Chapter XI Subchapter B. Managing the records includes, but is not limited to, secure storage, retrievability, and proper disposition of all federal records including transfer of permanently valuable records to NARA in a format and manner acceptable to NARA at the time of transfer. The agency is responsible for ensuring that the contractor is compliant with applicable records management laws and regulations through the life and termination of the contract.*[149]

NARA instructs that the use of this clause is "highly recommended," but it is not required, and there may be other ways to comply with the law. The key is to address records management requirements in advance so that TOS terms can be negotiated upfront.

---

[145] *Id.*
[146] *White Paper on Best Practice for the Capture of Social Media Records*, NAT'L ARCHIVES AND RECORDS ADMIN., at 10-20 (May 2013).
[147] *Id*. at 21.
[148] NARA Bull. 2011-02, at § 7 *supra* note 139. *See infra* Procurement and Terms of Service Agreements section for more information.
[149] *Id.*

Even if an OIG determines that content created through the use of new media does not constitute a Federal record, records management responsibilities still must be met. Specifically, electronic nonrecord materials must be readily identified and segregable from records, and nonrecord materials should be purged when no longer needed.[150] When considering using any new media, it is advisable to contact records management officers for their assistance in ensuring that all records management responsibilities are met.

Human Resources

Information and privacy issues may seem unrelated to human resources (HR), but in the world of social media they often connect. For example, when a hiring official prints out an applicant's social media social profile pages as part of the application process, this raises *Privacy Act* and records management issues. This section cover such issues as recruiting and hiring; new media passwords; workplace discrimination, harassment and retaliation claims; and employee actions that may give rise to adverse actions, such as for social media activities that undermine or adversely affect an OIG's mission. The following discussion briefly illustrates these areas of concern.

Recruiting and Hiring

Social media has become an increasingly popular way to recruit top talent to both government and the private sector. OIGs can use social networking websites to advertise jobs or answer questions about job postings on the Federal Government's official jobs website, USAjobs.gov. However, the recruiting and hiring process can bring problems if OIG staff are unaware of how to properly use social media. For example, some employers have started requesting applicants' and current employees' passwords to new media websites. At least four states have passed legislation making such requests illegal, and legislation is pending in other states.[151] In the Federal context, this practice would not only be impracticable but also likely illegal.[152]

We are not aware of a law that prohibits a hiring official from viewing an applicant's publicly accessible new media accounts as part of the hiring process. Information posted online for public viewing may be perceived simply as repackaged public information. In fact, depending on how and when it is done, an evaluation of an applicant's Internet footprint may be a useful component in determining his or her

[150] 36 C.F.R. § 1222.16.
[151] For a collection of state legislation that would prohibit requesting or requiring social networking passwords of applicants, students, or employees, see *Employer Access to Social Media Usernames and Passwords, 2012 Legislation*, Nat'l Conference of State Legislatures (Jan. 17, 2013), available at http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx.
[152] *See supra* First Amendment and Fourth Amendment sections.

fitness for Federal employment. However, OIGs should be aware that viewing an applicant's new media activity may lead to risks, including allegations of a *Privacy Act* violation or discrimination in the hiring process. The D.C. Circuit has held that merely performing an Internet search about an applicant would not constitute a *Privacy Act* violation, even if the searches were related to a person's First Amendment activities.[153] According to the D.C. Circuit, a violation occurs when a record is created; for instance, when there is a print-out or written annotation.[154]

A general social media search may reveal both factual and inaccurate information about a candidate. When information from social media websites is used to screen or openly eliminate a candidate from consideration, particularly if a decision to eliminate is based solely on the data found through social media content, an OIG is exposed to liability. For example, a hiring official's viewing of an applicant's social media profile may reveal that an applicant is pregnant, practices a certain religion, or graduated from college in a certain year. This is problematic if the applicant is not selected because the government cannot discriminate against an employee or applicant with respect to the terms, conditions, or privileges of employment on the basis of a protected class such as race, color, religion, sex, national origin, age, disability, marital status, or political affiliation.[155]

To defend against potential discrimination claims, an OIG manager who evaluates an applicant's new media activities and declines to interview or hire an applicant based on those activities should carefully document the basis for the decision. OIGs should carefully consider their reasons for considering the new media content objectionable and whether those reasons raise concerns that are relevant to the hiring process. For instance, they should ask themselves whether they disagree with the content for legitimate work-related reasons, or rather just do not approve of the views expressed. Does the applicant's speech indicate a suitability or background check issue? Does the speech cast doubt on whether the applicant would effectively promote the efficiency of OIG service? While answering these questions, it is important to remember an applicant's rights under the *Privacy Act*, not to mention antidiscrimination laws.[156]

---

[153] Gerlich v. Dept. of Justice, 828 F. Supp. 2d 284, 293-94 (D.D.C. 2011) (noting that, although "the Department of Justice's use of political or ideological affiliation in civil service hiring does not, in and of itself, violate the *Privacy Act*," it is "inappropriate, and could conceivably be the basis of some other claim").

[154] *Id.*

[155] Discrimination on these bases is prohibited by one or more of the following statutes: 5 U.S.C. § 2302(b)(1); 29 U.S.C. §§ 206(d), 631, 633a, 791; and 42 U.S.C. § 2000e-17.

[156] Section (e)(7) of the *Privacy Act* forbids agencies from maintaining records about how individuals express their First Amendment rights (subject to certain exceptions). *See supra* First Amendment section. Job applicants may file a claim for damages if the making of such a record "had an adverse effect on them as required by subsection (g)(1)(D) of the Act," Albright v. United States, 631 F.2d 915, 921 (D.C. Cir. 1980), and "'the agency acted in a manner which was intentional or willful.'" *Id.* (quoting 5 U.S.C. § 552a(g)(4)). In the D.C. Circuit, incorporation into a system of records is not necessary to trigger the *Privacy Act*. *Id.*

Finally, keep in mind that the sources considered in the hiring process may be considered agency records for *Privacy Act*, records management, and other purposes. Therefore, anyone authorized to use social media for hiring purposes should consult the OIG's privacy officer, counsel, and recordkeeping officer regarding potentially creating a record that is retrievable under the *Privacy Act*.

Workplace Discrimination Claims

In addition to potential pitfalls in the recruiting and hiring sphere, viewing the new media activity of current employees may lead to claims of discrimination, so OIGs should caution supervisors about the risks. Supervisors who share a social network with employees should not probe to find certain information through social media. For example, a supervisor who is connected on a social media network with an employee who posts about his or her serious health conditions inadvertently may learn about that employee's health. This is lawful.[157] However, the supervisor should not probe into health issues or conduct an Internet search on the employee in a way that likely will reveal genetic information to avoid claims of discrimination based on the *Genetic Information Nondiscrimination Act of 2008*, as amended.[158] It may be difficult for an OIG to argue successfully that it did not take action against an employee based on illegal grounds, if it is shown during discovery that a deciding official has viewed an employee's new media content purposefully to find such information.

Even if supervisors or management do not actively search new media for information about employees, they may become aware of information about an employee inadvertently through other employees' social media networks. Coworkers linked on social media platforms may print each other's postings and may choose to share them with management. OIGs should make sure that employees know to involve HR professionals and counsel regarding any allegation made involving social media.

Harassment and Hostile Work Environment Claims

A form of employment discrimination that violates Title VII of the *Civil Rights Act of 1964* (Title VII), as amended,[159] the *Age Discrimination in Employment Act of 1967*, as amended,[160] and the *Americans with Disabilities Act of 1990*, as amended,[161] harassment is unwelcome conduct that is based on race, color, religion, sex (including pregnancy), national origin, age, disability, or genetic information. Since 1986,

[157] *See* 29 C.F.R. § 1635.8(b)(1)(ii)(D). This social media situation is explicitly covered under the "inadvertent acquisition of genetic information" exception to the prohibition on requesting, requiring, or purchasing genetic information.
[158] 42 USCS § 2000ff-1, 29 C.F.R. § 1635.8(a).
[159] 42 U.S.C. §§ 2000e, et seq.
[160] 29 U.S.C. §§ 621-34.
[161] 42 U.S.C. §§ 12101, et. seq.

sufficiently "severe or pervasive" workplace harassment that "alter[s] the conditions of [the victim's] employment and create[s] an abusive working environment" has been recognized as an actionable claim against an employer under Title VII.[162] Known as a "hostile work environment" claim,[163] it is evaluated by "looking at all the circumstances" to determine whether the conduct was sufficiently severe or pervasive.[164] A single incident of harassment generally does not substantiate a hostile work environment.[165]

OIGs may not have considered whether social media activities could contribute to a hostile work environment claim, perhaps assuming that an abusive working environment must occur at the office to be actionable. But courts are examining whether the totality of the circumstances test may contemplate harassment that occurs after hours or away from the office. Federal circuit courts are split on this issue, with the First, Second, Seventh, and Eighth Circuit Courts of Appeals indicating that harassment conducted outside the workplace counts towards the totality of the circumstances for purposes of a hostile work environment claim.[166] Courts may consider social media harassment as part of the totality of the circumstances test.[167]

Arguably, as the concept of the federal workplace expands to include more teleworking, professional and personal boundaries increasingly blur, and employees increasingly use social media both for personal and professional purposes, an OIG's potential liability under Title VII may grow. This is an area of law to follow.

Retaliation Claims

Retaliation against an employee or applicant for making a protected disclosure is prohibited by Federal law.[168] In addition, the Federal Government cannot retaliate against an employee or applicant because that individual exercises his or her rights under any of the Federal antidiscrimination or whistleblower protection laws.[169] If an

[162] Meritor Sav. Bank v. Vinson, 477 U.S. 57, 64-67 (1986).
[163] *Id*. at 66.
[164] Harris v. Forklift Systems, Inc., 510 U.S. 17, 23 (1993).
[165] Faragher v. City of Boca Raton, 524 U.S. 775, 778 (1998) ("[S]imple teasing,' offhand comments, and isolated incidents (unless extremely serious) will not amount to discriminatory changes in the 'terms and conditions' of employment.'" (quoting Oncale v. Sundowner Offshore Serv., Inc., 523 U.S. 75, 81-82 (1998))).
[166] *See* Jeremy Gelms, *High-Tech Harassment: Employer Liability Under Title VII for Employee Social Media Misconduct*, 87 Wash. L. Rev. 249, 259 (2012) (citing Crowley v. L.L. Bean, Inc., 303 F.3d 387, 409–10 (1st Cir. 2002); Ferris v. Delta Airlines, Inc., 277 F.3d 128, 135 (2d Cir. 2001); Lapka v. Chertoff, 517 F.3d 974, 983 (7th Cir. 2008); Doe v. Oberweis Dairy, 456 F.3d 704, 715 (7th Cir. 2006); Dowd v. United Steelworkers of Am., 253 F.3d 1093, 1102 (8th Cir. 2001)).
[167] *Id.* at 271 (citing Blakey v. Continental Airlines, Inc., 751 A.2d 538 (2000) ("Although the electronic bulletin board may not have a physical location [at the office] it may nonetheless have been so closely related to the workplace environment . . . that a continuation of harassment on the forum should be regarded as part of the workplace."); Amira-Jabbar v. Travel Services, Inc., 726 F. Supp. 2d 77 (2010) (social media harassment sufficiently work-related to be considered among all the circumstances)).
[168] 5 U.S.C. § 2302(b)(8).
[169] 5 U.S.C. § 2302(b)(9).

OIG learns about an employee's complaint of retaliation, either by monitoring the employee's social media activity on a government computer or through a social network that another OIG employee shares with the aggrieved employee, the OIG may be vulnerable to a retaliation claim if the employee later suffers an adverse employment decision. The *Whistleblower Protection Enhancement Act of 2012*[170] recently expanded its protection of Federal employees from reprisal if they disclose misconduct to coworkers or supervisors, disclose the consequences of a policy decision, or, under certain conditions, blow the whistle while carrying out their job duties – even if they are not the first person to disclose misconduct.[171] Therefore, a tweet about retaliation or even a message through a social media account to a supervisor or coworker, made on or off duty, may constitute a protected disclosure under the *Whistleblower Protection Act*.

Taking Adverse Action

At some point, an OIG may learn through social media that an employee has violated the law or OIG policy. For instance, an employee may have disclosed nonpublic information or posted photos from a hockey game that the employee attended while on sick leave.[172] Or perhaps an employee posted or tweeted excessively while on duty, or violated another workplace policy involving social media. For whatever reason, an OIG may wish to discipline the employee based on information gleaned from social media.

Federal agencies are starting to include social media activities in disciplinary actions, but it is wise to be cautious.[173] Federal law permits an agency to take adverse action against an employee "only for such cause as will promote the efficiency of the service," including circumstances involving off-duty activities.[174] Thus, it is important that an OIG establish clear, predetermined standards as to when private misconduct in connection with the use of social media rises to the level of misconduct that adversely affects an OIG's efficiency of service.

Since "agenc[ies] [have] the burden of proof to establish that [an] employee's discipline will 'promote the efficiency of the service,'"[175] OIG policies should give examples of actions considered to be misuse of social media. In addition, they should spell out the discipline that will be administered in response to such actions and how such discipline promotes the efficiency of the OIG service. When defining social media misconduct, it is

[170] Pub. L. No. 112-199, 126 Stat. 1465 (2012).
[171] *Id*. 5 U.S.C. § 2302(f).
[172] *See* Hunter v. Dep't of Navy, 2011 Merit Systems Protection Board (MSPB) Lexis 3159 (May 20, 2011) (allegation that Navy police officer appellant called in sick but posted information on Facebook showing that he had watched the Superbowl).
[173] *See* Vidal v. Army, 2011 MSPB Lexis 4788 (Aug. 5, 2011) (involving agency removal of employee because of alleged anxiety-producing comment on Facebook that was reported at work); Shannon v. VA, 2013 MSBP Lexis 563 (Jan. 31, 2013) (affirming agency decision to remove employee for exchanging personal Facebook messages with veteran resident, in violation of policy).
[174] 5 U.S.C. § 7513(a).
[175] Doe v. Dep't of Justice, 565 F.3d 1375, 1379 (Fed. Cir. 2009).

critical that OIGs include only actions that would impact job performance directly and in obvious ways.[176] That said, the Merit Systems Protection Board and the Federal Circuit generally have held that off-duty activities can lead to discipline when they could cause the public or coworkers to question or lose confidence in the Federal agency involved.[177]

One of the factors making social media so complicated is that it requires employees to decide among apparently simple options, some of which may pose problems. For example, regarding employment status, employees may choose to identify themselves on their personal social media websites as employees of specific OIGs, generically as a Federal employee or by profession, or not list their employment status at all. Employees who identify their specific workplace open themselves up to potential ethics and *Hatch Act* violations, if their posts could be construed as official endorsements or improper political activity. Some senior or publicly known employees may be so well-known that they cannot successfully hide their employer and position, practically eliminating the chances of successfully maintaining a purely "personal" social media account. As for privacy settings, employees may choose to restrict access to certain people or groups, or open everything to anyone who wishes to see.

OIGs must create a social media policy that considers these and other factors in assessing the risks that an employee's potentially problematic speech or content may pose, keeping in mind that if required to defend that policy in a personnel action, the OIG will need to establish that the actions constituting the violation "could rationally be considered likely to discredit" the OIG.[178]

In short, an OIG's adoption of standards that reflect a clear nexus between misuse of social media and efficiency of service to the OIG will provide a uniform basis for evaluating employee conduct. Furthermore, including these standards in OIG policy (along with examples of each) will put employees on notice of prohibited practices in connection with social media use.

In summary, new media is an effective tool for both employers and employees when used properly, but both groups must be aware of the potential pitfalls. Strong employer

[176] *Id.* at 1380-81 (citing Brown v. Dep't of the Navy, 229 F.3d 1356, 1360 (Fed. Cir. 2000) and Bonet v. U.S. Postal Serv., 661 F.2d 1071, 1078 (5th Cir. 1981) (noting that it is insufficient to rely on internal regulations that generally proscribe certain employee conduct (e.g., "immoral" or "disgraceful" conduct) as proof of the required nexus between off-duty dishonesty/immorality and the efficiency of the service)).

[177] *E.g.*, Stump v. Dep't of Transp., 761 F.2d 680, 681-82 (Fed. Cir. 1985) (upheld MSPB decision sustaining removal of employee for off-duty cocaine use).

[178] Major v. Hampton, 413 F. Supp. 66, 67 (E.D. La. 1976). When determining if a particular action would satisfy this test, OIGs must consider "the nature of the acts, the circumspection or notoriety with which they are performed, and the atmosphere of the community in which they take place." *Id*. at 69. Note that the third consideration promoted by the court is an allusion to the obscenity test in Miller v. California, 413 U.S. 15, 24 (1973), which dictates that obscenity should be defined according to "contemporary community standards."

guidance and circumspect employee activity will go a long way in preventing damage to the employer-employee relationship.

Ethics

One area with potential to raise many HR issues is the field of ethics. Because new media allows more opportunities for employees to interact and express themselves, it presents a potential minefield of ethics violations. This section covers impartiality and endorsements; use of government resources; outside activities; nondisclosure of nonpublic information; the *Anti-Lobbying Act*; the *Hatch Act*; and appropriations restrictions.

Ethics Overview

All Federal employees must comply with Federal ethics laws.[179] The standards for ethical conduct cover the basic ethical obligations of public service, including rules regarding gifts from outside sources and between employees, conflicting financial interests, impartiality in performing official duties, outside employment and activities, post-employment, and misuse of position.[180] Based on 14 principles, the standards are designed to instill public faith in public servants. They apply to employee communications and conduct regardless of the medium, so it follows that they apply to the use of new media.

Overview of Impartiality and Endorsements

New media, and social media in particular, offers OIGs in an official capacity and employees in an unofficial, off-duty capacity the opportunity to "endorse" people, enterprises, and ideas. For example, Twitter accounts allow users to retweet messages, which may imply an endorsement of the message.[181] Facebook allows users to "like" other users' pages, posts, and links. And LinkedIn allows users to recommend or "endorse" others' work and expertise. Merely subscribing to or "following" an individual or organization's social media site could appear to be an endorsement.

Employees and their employing OIGs should be aware that Federal ethics rules require impartiality and prohibit employees from endorsing products, services, or enterprises in the performance of their official duties or while engaging in activity that creates the

[179] Most of the ethics laws are found in Sections 202 to 209 of Title 18 of the U.S. Code and in Exec. Order No. 12,674, 54 Fed. Reg. 15,159 (Apr. 12, 1989), *modified by* Exec. Order No. 12,731, 55 Fed. Reg. 42,547 (Oct. 17, 1990). The executive order is implemented by regulations at 5 C.F.R. § 2635.
[180] 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.
[181] An OIG may state on its profile that "retweet does not mean endorsement," as other Twitter users do, but tweeting from an official account nonetheless may create the impression of endorsement.

appearance that the endorsement is somehow related to their official position. Specifically, the rules require employees to—

- "[A]ct impartially and not give preferential treatment" to private organizations or individuals;[182]
- Try to "avoid any actions creating the appearance" that they are violating laws or ethical standards;[183]
- Not use their public office to endorse "any product, service, or enterprise,"[184] except when an exception applies;[185] and
- Not use their public position or title or any authority associated with their public office "in a manner that could reasonably be construed to imply" that the government endorses their personal activities or those of another.[186]

Impartiality and Endorsements – Unofficial Employee Use

Based on the ethics rules on impartiality and endorsement, an employee may list his or her OIG position on a professional social media networking site but should be cautious about making recommendations in connection with the account. An employee is prohibited from recommending companies, products, or services in an official capacity but is permitted to make recommendations in a purely personal capacity. The safest option is to avoid such endorsements altogether. However, an employee identified by his official title may write a recommendation for or "endorse" someone on LinkedIn under certain circumstances. An employee may make a recommendation in his official capacity based upon his personal knowledge of the ability or character of someone with whom he has dealt in the course of Federal employment or whom he is recommending for Federal employment.[187] Writing a recommendation, in an official capacity, on social media for a government contractor would likely violate the Standards of Conduct.

Another opportunity to run into an endorsement pitfall concerns fundraisers through social media, sometimes referred to as "social fundraisers." An employee may engage in a fundraising event not sponsored by the government, but may not allow his or her title, position, or any authority connected with OIG to further the fundraiser.[188] Further,

[182] 5 C.F.R. § 2635.101(b)(8).
[183] *Id*. at § 2635.101(b)(14).
[184] *Id*. at § 2635.702.
[185] *Id*. at § 2635.702(c).
[186] *Id*. at § 2635.702(b).
[187] *Id*.
[188] *Id*. at § 2635.808(c).

an employee engaging in fundraising in a personal capacity via social media may not solicit funds or other support from a subordinate or prohibited source.

Impartiality and Endorsements – Official OIG Use

With respect to *official* OIG social media activity, OIGs should have a policy governing the entities that the OIG "likes," "follows," or "recommends." An OIG social media policy should inform employees of their ethical duties not to endorse private products, services, or programs in their official capacity, and instruct them not to associate their personal opinions with their public position. OIGs should monitor the activity of employees in charge of OIG official social media platforms to ensure compliance.

Generally, in the absence of statutory authority to endorse certain products, programs, or services, an OIG may choose to like, endorse, or follow only other governmental agencies or officials to avoid the appearance of improper endorsements.[189] Just accepting a "friend" or other social media connection request from a public user may be fine, but the OIG should not proactively "friend," "follow," or "like" public users.[190] An OIG employee using social media in an official capacity also should avoid direct endorsements. For example, the employee should not post a statement saying that the OIG uses a particular provider because it is "the best platform for public communication." However, the employee may post a statement such as "OIG just negotiated a terms of service agreement with [social media provider], which will provide OIG with a platform to communicate with the public," which is a statement of fact and not an opinion or endorsement.

Sometimes, however, an OIG's mission might require following news of state and local governments, or nonprofit organizations on Twitter or other social media platforms. For example, an OIG that oversees a grant-making agency or is involved in emergency preparedness may justify following certain relevant entities. If an OIG's mission could benefit from following major news outlets, it is advisable for the OIG to follow all major networks rather than one so that no preference is indicated.

OIGs should not allow third-party social media providers to use their logos or seals, nor should OIGs endorse or promote non-Federal logos or seals. Doing so may violate Federal contracting regulations requiring the government to treat all potential contractors with impartiality to allow for fair competition.[191] It also may violate the

[189] For example, 42 U.S.C. § 6294a requires the Department of Energy and the Environmental Protection Agency to endorse specific products and services.
[190] CIO Council Privacy Best Practices, #4(b)(iii), *supra*, note 83. The CIO Council suggests that a statement be included in the PIA and on the social media account page to inform users that the acceptance of a friend or other social media connection request does not indicate endorsement.
[191] 48 C.F.R. § 3.101-1.

general ethical principle requiring employees to be impartial and avoid giving preferential treatment.[192] One way to address potential problems is to use a disclaimer on all OIG-sponsored social media platforms stating that the OIG does not endorse any nongovernment websites, companies, or apps. An OIG also may wish to provide a link on its website as to why the OIG uses certain social media apps, and encourage readers to suggest other products. Finally, if links to an OIG's third-party websites are provided, the OIG should consider adding a banner or disclaimer advising individuals that they are leaving the OIG website and entering the third-party website, and the OIG does not endorse any commercial products that may be advertised with the website.[193] OGE's online disclaimer contains the following information regarding endorsements:

> *Reference in this site to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public, and does not constitute endorsement, recommendation, or favoring by the Department of Justice.*
>
> *OGE does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained on a linked website; does not endorse the organizations sponsoring linked websites; does not endorse the views they express or the products/services they offer. . . .*[194]

Employee Use of Government Resources

Federal employees always have a duty to protect and conserve Federal resources and to put forth an honest effort while on duty.[195] However, most OIGs have a "limited use policy" that allows employees to use government resources, including government computers and electronic devices, for personal purposes. This use is restricted, as the name implies, and requires that employees comply with legal and policy guidelines. Typical restrictions are that use should occur at times that do not interfere with an employee's duties, should not trigger more than nominal increases in cost, and should not violate applicable laws or regulations. An employee who spends two hours a day updating social networking websites in a personal capacity on a government electronic device would be violating these rules.

[192] 5 C.F.R. § 2635.101(b)(8).
[193] The banner should also state that the OIG's privacy policy does not apply on third-party websites and applications.
[194] *See* OGE Disclaimer of Liability, *supra* note 110.
[195] 5 C.F.R. §§ 2635.101(b)(5), (b)(9), 2635.704, 2635.705.

Restrictions on Outside Activities

Federal ethics regulations dictate that an employee's outside employment and activities may not conflict with their official duties.[196] Supplemental agency ethics regulations, for agencies that have them, often include agency-specific restrictions on outside activities.[197] So, for example, while maintaining a personal blog is allowable, employees who choose to list their position or title should only cite it as one of several biographical details, and include a disclaimer stating that the views presented represent the blogger's personal views and not those of the OIG. Also, an employee should not blog or conduct other social media activities from their government computers, beyond that allowed by a "de minimis" use policy.

Nondisclosure of Nonpublic Information

Federal ethics rules forbid Federal employees from using, or allowing someone to use, nonpublic Government information to further their own private interests or the private interests of others.[198] As defined by ethics regulations, nonpublic information is information that an employee gains by reason of Federal employment and that he or she knows or reasonably should know has not been made available to the general public[199] It includes information that is exempt from disclosure under the FOIA, or otherwise protected by EO or regulation, and information designated confidential by an agency.[200] OIG employees need to be particularly careful with social media, where it is easy to click and disclose but practically impossible to retrieve and delete. Depending on the nature of the information, disclosing via social media might violate not just the Standards of Conduct, but also various Federal statutes.

Prohibition of Lobbying

Social media platforms are effective ways to get a particular message across and communicate ideas to those who are unreachable through traditional methods. However, Federal agencies have a duty of political impartiality and must be conscientious of the *Anti-Lobbying Act*, which prohibits Federal funds from being used to directly or indirectly lobby Congress or any government official.[201]

[196] *Id*. at § 2635.802.
[197] OGE's website provides links to all supplemental agency ethics regulations. See *Agency Supplemental Regulations*, OFF. OF GOV. ETHICS, http://www.oge.gov/Laws-and-Regulations/Agency-Supplemental-Regulations/Agency-Supplemental-Regulations/ (last visited Aug. 16, 2013).
[198] 5 C.F.R. § 2635.703.
[199] 5 C.F.R. §2635.703(b).
[200] 5 U.S.C. § 552.
[201] 18 U.S.C. § 1913.

Anti-Lobbying Act violations can occur inadvertently through official or unofficial new media use. Employees using new media to encourage the public to pressure Congress to support any legislation, law, or policy—whether advocating an agency position or not—may be found to engage in "grass roots lobbying." These activities may violate the *Anti-Lobbying Act* if done on official time, since Federal salaries come from appropriated funds.[202]

To combat the risk of inappropriate lobbying, OIGs should train employees regarding this issue. Additionally, OIGs should develop understanding of what constitutes prohibited lobbying activity in the realm of social media and provide employees with adequate training on the basic principles of the *Anti-Lobbying Act*. As with many other areas of the law, staying abreast of *Anti-Lobbying Act* developments as applied to new media will greatly help to mitigate potential violations.

Prohibition of Partisan Activities

OIGs need to be aware of the *Hatch Act*'s ban on Federal employees' partisan political activities.[203] According to the Office of Special Counsel's frequently asked questions (FAQ) on social media and the *Hatch Act*, the basics for "less restricted" employees are as follows:[204]

- If a Federal employee has listed his official title on his Facebook profile, he or she may also fill in the "political views" field.

- Federal employees are prohibited from advocating for or against a political party, partisan political group, or candidate for partisan public office through social media while on duty or in the workplace. However, doing so off duty and away from the Federal workplace would not violate the *Hatch Act*, as long as employees do not refer to their official titles or positions.

- Employees may not solicit, accept, or receive political contributions, or suggest or ask anyone to contribute to a political party, partisan political candidate, or partisan political group. This restriction applies in the social media world.

- Employees should not provide links to the contribution page of any of those entities' websites.

[202] *See* Application of 18 U.S.C. § 1913 to "Grass Roots" Lobbying by Union Representatives, 29 Op. O.L.C. 1 (Nov. 23, 2005).
[203] 5 U.S.C. §§ 7321-26.
[204] *Frequently Asked Questions Regarding Social Media and the Hatch Act*, U.S. OFF. OF SPECIAL COUNSEL (Apr. 4, 2012), available at http://www.osc.gov/documents/hatchact/federal/Social%20Media%20and%20the%20Hatch%20Act%202012.pdf.

- Supervisors sharing social media networks with subordinates generally may advocate for or against a political party, partisan political group, or candidate for partisan public office via social media but may not direct any message toward a specific subordinate employee or to a subset of friends that includes subordinates.

- Employees are not liable for their social media contacts' speech but should not "like," "share," or "retweet" speech that the employee would be prohibited from stating himself.

- Official social media accounts must be politically neutral. In other words, employees managing the OIG's accounts may not "like" or "follow" political parties, or include information on such groups.

Some Appropriations Restrictions

Some OIGs have held digitized "town halls," which allow an Inspector General or senior staff to address questions in real time. Others use blogs, video and audio sharing platforms, and other social media to push out their message. Among the benefits of engaging social media in this way is that an OIG can control its message and respond to any negative publicity immediately. When pushing out a message, however, OIGs need to be careful to avoid propaganda. In the past 50 years, GAO has noted that one of the main targets of the publicity or propaganda prohibition is when the "obvious purpose is 'self-aggrandizement' or 'puffery.'"[205] By focusing on legitimate informational activities,[206] an OIG fulfills its duty to inform the public regarding its policies, while avoiding puffery.[207] Using OIG resources in explanation and defense of the OIG's policies—even in the absence of specific direction or a mandate—is allowable.[208] GAO has consistently held that public officials may report on their activities and programs, may justify those policies to the public, and may rebut attacks on those policies.[209]

[205] *E.g.*, Application for Anti-Lobbying Restrictions to HUD Report Losing Ground, B-284226.2, 2000 WL 1193462 (Comp. Gen. Aug. 17, 2000); Medicare Prescription Drug, Improvement, and Modernization Act of 2003, B-302504, 2004 WL 523435 (Comp. Gen. Mar. 10, 2004). GAO has defined self-aggrandizement as "publicity of a nature tending to emphasize the importance of the OIG or activity in question." Restriction Violations on the Use of Appropriations in a Press Release by the Office of Personal Management, B-212069 (Comp. Gen. Oct. 6, 1983) (quoting 31 Comp. Gen. 311 (1952) (GAO's first decision interpreting the publicity or propaganda prohibition). For example, an OIG would be prohibited from using appropriated funds to issue a press release to persuade the public as to its importance as a government OIG but not prohibited from providing legitimate information, such as on pending legislation. *Id.* (finding OPM press releases informing the public of the Administration's position on pending legislation unobjectionable).

[206] Benjamin S. Rosenthal, House of Representatives, B-184648, 1975 WL 9457 (Comp. Gen. Dec. 3, 1975) (discussing an OIG's "legitimate interest in communicating with the public").

[207] Medicare Prescription Drug, Improvement, and Modernization Act of 2003, B-302504, 2004 WL 523435 (Comp. Gen. Mar. 10, 2004) (citing B-130961, Oct. 26, 1972) (stating that "OIGs have a general responsibility, even in the absence of specific direction, to inform the public of the OIG's policies").

[208] *Id*.

[209] *Id*. (citing B-223098, Oct. 10, 1986) (stating that "public officials may report on the activities and programs of their OIGs, may justify those policies to the public, and may rebut attacks on those policies").

Procurement and Terms of Service Agreements

Even though many social media services are free, OIGs still need to be aware of procurement issues, whether at the initial stage of choosing a provider or negotiating a TOS or user agreement. The key is to negotiate a TOS upfront that considers all legal, privacy, and information security requirements. This section addresses no-cost agreements, and issues that TOS agreements raise, including potentially problematic clauses on indemnification, choice of law and forum, confidentiality, and advertising.

No-Cost Agreements

The *Competition in Contracting Act of 1984*, as amended, applies to Federal agency procurements for property or services, and generally requires full and open competition.[210] However, since much of the new media available today is provided for free, procurements are often set up as no-cost agreements. A no-cost agreement is a "formal arrangement between a government entity and a vendor under which the government makes no monetary payment for the vendor's performance."[211] GAO guidance advises that determining whether competition requirements apply to a no-cost agreement depends on the agency involved.[212] GAO ultimately concluded that the *Competition in Contracting Act of 1984* does not apply to no-cost agreements of military agencies but does apply to no-cost agreements of civilian agencies.[213]

No-cost agreements do not violate the *Antideficiency Act* because "[s]ervices performed pursuant to a formal contract, in which the OIG has no financial obligation and the contractor has no expectation of payment from the government, are not 'voluntary' within the meaning of the prohibition."[214] Therefore, as long as an OIG enters into a formal no-cost agreement with a social media provider that clearly states that the OIG has no financial obligation and that the social media provider has no expectation of payment from the OIG, the no-cost agreement will not violate the *Antideficiency Act*.

[210] 41 U.S.C. § 3301.
[211] No-Cost Contracts for Event Planning Services, B-308968, 2007 WL 4226075 (Comp. Gen. Nov. 27, 2007) (citing General Services Administration and Real Estate Brokers' Commissions, B-302-811 (Comp. Gen. July 12, 2004)).
[212] *GAO, No-Cost Contracts: Frequently Asked Questions*, GOV'T ACCOUNTABILITY OFF. (Mar. 13, 2008), #5, *available at* http://www.gao.gov/special.pubs/appforum2008/nocostcontracts.pdf [hereinafter GAO FAQ].
[213] *Id*.
[214] No-Cost Contracts for Event Planning Services, B-308968, 2007 WL 4226075 (Comp. Gen. Nov. 27, 2007). The Antideficiency Act prohibits voluntary services because they may generate claims for compensation that may exceed an OIG's appropriations. See 31 U.S.C. § 1342 ("An officer or employee of the United States Government . . . may not accept voluntary services . . . or employ personal services exceeding that authorized by law except for emergencies involving the safety of human life or the protection of property.").

The Federal Acquisition Regulation (FAR) does not apply to acquisitions of free media services, whether by a defense or civilian agency, because it applies only to government acquisition of supplies or services with appropriated funds.[215] As with any other government expenditure, though, if the new media platform will require appropriated funds, the FAR applies to that procurement.

User Agreements and Terms of Service

OIGs should not sign a boilerplate TOS agreement with a new media provider but rather should negotiate the terms. OLC has determined that the standard of consent to an online TOS is the same as for traditional principles of contract law.[216] As a result, consent to an online TOS "turns on whether the web user had reasonable notice of and manifested assent to the online agreement."[217] OIG employees need to read the agreements, whether they are "clickwrap" or "browsewrap,"[218] and avoid accepting standard "click-through" user agreements on most new media websites, as they usually contain provisions that are problematic for the Federal Government and may lead to a violation of the law.[219]

In 2009, the General Services Administration (GSA) began negotiating TOS agreements with various new media platforms for Federal government use. GSA publishes on www.howto.gov/tos a list of Federal-compatible TOS agreements that address many of the major legal issues (e.g., indemnification, liability, choice of law, advertising) that may arise. Although it may be tempting to use these templates as-is, OIG staff should review them for their own needs and negotiate with the provider as necessary.

When using www.howto.gov/tos to begin the process of enrolling in a new media program, OIGs should be aware that GSA generates an email to the parent OIG's point of contact for approval, if applicable. Some parent agencies may try to prevent an OIG from starting and maintaining its own account. An OIG seeking to utilize a new media platform will need to work with the parent OIG point of contact to explain that (whether the parent OIG has its own account with the new media provider in question or not) the OIG account will be separate from any parent agency account. An OIG might need to

[215] 48 C.F.R. §§ 1.104, 2.101; *See also* Fidelity and Casualty Company of New York, B-281281, 1999 WL 22661 (Comp. Gen. Jan. 21, 1999); GAO FAQ, *supra* note 212, at #5.
[216] *The Anti-Deficiency Act Implications of Consent by Government Employees to Online Terms of Service Agreements Containing Open-Ended Indemnification Clauses*, OFF. OF LEGAL COUNSEL (Mar. 27, 2012), available at http://www.justice.gov/olc/2012/aag-ada-impls-of-consent-by-govt-empls.pdf.
[217] *Id*.
[218] "Clickwrap" agreements require the user to take an affirmative action, such as checking a box or clicking an "I accept" or "I agree" button. "Browsewrap" agreements are passive and do not require the user to give express consent.
[219] Note, however, that some social media providers have changed their basic TOS to be compatible with Federal OIG requirements.

clarify that, due to independence requirements, the TOS agreement will be reviewed and approved by OIG counsel, rather than agency counsel.

Indemnification Clauses

Service providers generally include indemnification clauses in TOS agreements. A standard indemnification clause might state that, if liability arises connected to the social media content or activities, the account holder must indemnify and hold the provider harmless from and against all damages, losses, and expenses of any kind. It might include reasonable legal fees and costs.

Agreeing to such an open-ended, unrestricted indemnification clause would violate the *Antideficiency Act* because employees may not "make or authorize an expenditure or obligation exceeding an amount available in an appropriation or fund for the expenditure or obligation."[220] The OLC determined that an employee with actual authority to contract on behalf of the government violates the *Antideficiency Act* by entering into such an obligation, whereas an employee without contracting authority does not.[221] This applies whether the service is free or fee-based.

To remedy any violations, GSA has negotiated indemnification clauses in TOS agreements with numerous providers. Here is one example:

> 3. (b) Indemnity. The indemnity provision in the Terms of Use is hereby deleted in its entirety and replaced with the following:
>
> *Disclaimer. You agree that your account on the [social media provider] service will serve as an additional distribution channel for government information, but in no event will serve or be represented as the official site or homepage for Government Entity. To help convey this message, you will maintain the following message in a prominent location on your [social media provider] page: "If you're looking for the official source of information about [Government Entity], please visit our homepage at [URL Link]."*[222]

GSA's model TOS includes the following indemnification language:

---

[220] 31 U.S.C. § 1341(a)(1)(A).

[221] *The Anti-Deficiency Act Implications of Consent by Government Employees to Online Terms of Service Agreements Containing Open-Ended Indemnification Clauses*, OFF. OF LEGAL COUNSEL, (Mar. 27, 2012), available at http://www.justice.gov/olc/2012/aag-ada-impls-of-consent-by-govt-empls.pdf. If an employee without the authority to contract on behalf of the agency signs such a TOS, however, OLC determined that that would not violate the Antideficiency Act. According to FAR provision 48 C.F.R. § 4.101, only contracting officers have the authority to bind an agency to a contract.

[222] *Negotiated Terms of Service Agreements*, GEN. SERV. ADMIN., http://www.howto.gov/web-content/resources/tools/terms-of-service-agreements/negotiated-terms-of-service-agreements (last visited Aug. 16, 2013) [hereinafter GSA TOS Amendments].

> ***Indemnification, Liability, Statute of Limitations*****:** *Any provisions in the TOS related to indemnification and filing deadlines are hereby waived, and shall not apply except to the extent expressly authorized by law. Liability for any breach of the TOS as modified by this Amendment, or any claim arising from the TOS as modified by this Amendment, shall be determined under the Federal Tort Claims Act (FTCA), or other governing Federal authority. Federal Statute of Limitations provisions shall apply to any breach or claim.*

The following indemnification language may be added to supplement the language contained in GSA's model TOS:

> *As an OIG of the United States Government, [OIG] is self-insured. Pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. §§ 1346(b), 2671-80, the exclusive remedy for any negligent or wrongful act or omission on the part of its employees, when acting within the scope of their employment, shall be an action against the United States under the FTCA. As such, [OIG] acknowledges that liability for any acts or omissions on the part of its employees shall be determined pursuant to the FTCA.*

By negotiating with providers for the deletion of open-ended indemnification language, OIGs can ensure that TOS agreements they enter into with social media providers comply with the *Antideficiency Act*.

Choice of Law/Choice of Forum Clauses

TOS agreements also generally include choice of law and choice of forum clauses that require disputes to be resolved in a specific forum, most often a state court, or pursuant to a specific state's law. These clauses violate the sovereign immunity doctrine and 28 U.S.C. §§ 1346 and 1491, which govern jurisdiction in cases involving the United States as defendant.[223] OIGs should also be aware of the possible applicability of the *Contracts Dispute Act of 1978*, as amended; the FTCA; and the *Tucker Act*.

Boilerplate choice of law and choice of forum clauses may state the following:

> *You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to [social media provider] exclusively in a state or Federal court located in [County]. The laws of [State] will govern this Statement/Agreement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal*

[223] Sovereign immunity is a legal doctrine granting the Federal Government immunity from lawsuits unless it has consented to being sued. Gray v. Bell, 712 F.2d 490, 509-10 (D.C. Cir. 1983).

jurisdiction of the courts located in [County, State] for the purpose of litigating all such claims.

To avoid violations of applicable law, GSA has negotiated with service providers to amend such language. GSA's negotiated TOS agreement with one social media provider includes the following language:

> 3(a) Governing Law and Liability of Government Entity. The provision in the Terms of Use that governs the jurisdiction, venue and choice of law in the resolution of any claim, cause of action or dispute arising out of your use of [social media site] is hereby replaced with the following:
>
> *You and [social media site] will endeavor to resolve any claims, causes of action or disputes in an amicable fashion. Any claim, cause of action or dispute that arises from these Terms of Use will be governed, interpreted and enforced in accordance with the laws of the United States of America. In the absence of federal law, the laws of [State] will apply. The liability of Government Entity and its obligations to Company resulting from any breach by Government Entity of any of the provisions of this Terms of Use or any claim, cause of action or dispute arising from this Terms of Use will be determined under the Contract Disputes Act, the Federal Tort Claims Act, the Tucker Act, or any other applicable law.*[224]

GSA's model TOS includes the following choice of law language:

> ***Governing law***: *Any arbitration, mediation or similar dispute resolution provision in the TOS is hereby deleted. The TOS and this Amendment shall be governed by and interpreted and enforced in accordance with the laws of the United States of America without reference to conflict of laws. To the extent permitted by federal law, the laws of the State of [Company to insert name of state if one is mentioned in its TOS] (excluding [Company's state] choice of law rules) will apply in the absence of applicable federal law.*[225]

As with the indemnification language above, OIGs should determine whether GSA-negotiated language with regard to choice of law and forum fits their needs. If an OIG negotiates with a service provider, then at a minimum the choice of law and forum clauses should establish that Federal law applies to the agreement, not state law, since Federal courts have exclusive jurisdiction over the Federal Government.

[224] *See* GSA TOS Amendments, *supra* note 222.

[225] *Amendment to [Name of Company] Terms of Service Applicable to U.S. Government Users/Members*, GEN. SERV. ADMIN., available at http://www.howto.gov/sites/default/files/model-amendment-to-tos-for-g.pdf (last visited Aug. 16, 2013).

Confidentiality Clauses

Some new media providers include confidentiality clauses in their user agreements. As discussed above, the FOIA provides individuals with a right, enforceable in court, to request and obtain access to Federal agency records, except to the extent that records or portions of records are protected from public disclosure by a statutory exemption or exclusion.[226] Since an OIG's use of new media can result in the creation of records, an OIG may be required under FOIA to disclose such information in violation of any confidentiality clause. An OIG may also be required to produce records created through the use of new media in response to a *Privacy Act* request, a subpoena, or a discovery order. If a confidentiality clause exists in a new media provider's TOS agreement, it is advisable to ensure that any TOS be amended to recognize that the OIG will maintain confidentiality "to the extent permitted by law."

Advertising Clauses

Increasingly, social media websites include paid advertising on the pages of their subscribers, and a boilerplate TOS agreement may include a clause requiring the subscriber to authorize this practice. However, ads on an OIG's social media page create a risk of violating regulations prohibiting employees from using or allowing the use of their public office to endorse any product, service, or enterprise.[227] Whether explicitly authorized by the subscribing OIG or not, ads on OIG-sponsored new media could be construed as an endorsement of the advertised product or service. To prevent violations, TOS agreements should be carefully examined for provisions concerning advertising, and modifications should be negotiated as necessary. For example, a GSA-approved TOS agreement for Federal agencies contains the following provision:

> *Company hereby agrees not to serve or display any third party commercial ads or solicitations on any pages within the Company website displaying content created by or under the control of the Agency, provided that your sole remedy for [Company's] breach hereof shall be to terminate your use of the website. This exclusion shall not extend to house ads, which Company may serve on such pages in a non-intrusive manner.*[228]

This provision allows the new media provider to place one sort of advertisement on Federal Government pages—"house advertisements" for its own services. Although house ads may be permissible, OIGs should not agree to a TOS that allows advertising from other sources. Table 2 shows possible ways to address TOS issues:

[226] 5 U.S.C. § 552. *See supra* Information and Privacy section.
[227] 5 C.F.R. § 2635.702.
[228] *See* GSA TOS Amendments, *supra* note 222.

Table 2: TOS Issues

Clause	Issue	Possible Fix
Indemnification	User (OIG) agrees to reimburse the provider for damages to third parties. Violates *Antideficiency Act*.	Incorporate Federal government liability limits from *Federal Tort Claims Act*.
Choice of Law	Contrary to sovereign immunity doctrine.	Change to incorporate Federal laws, such as *Contract Disputes Act*, *Federal Tort Claims Act*, and the *Tucker Act.*
Choice of Forum	Contrary to sovereign immunity doctrine.	Change clause to reflect "any competent Federal court."
Unilateral Changes	Provider reserves right of unilateral change to TOS, after notice on website.	Require notification period with time limit for OIG to concur or terminate agreement.
Use of Agency Name/Seal/Logo	May create the appearance of endorsement.	Allow provider to use OIG name or seal only to state that it uses the provider's service (factual statement). Forbid provider from stating or implying that OIG endorses the service, or from using OIG logo or seal in ads.
Confidentiality	Possible inconsistency with *Privacy Act*, FOIA, or litigation requirements.	Incorporate statutory disclosure requirements.
Advertisements	May create apparent endorsement of advertised service or product.	Change clause to prohibit third-party ads or solicitations.

Intellectual Property Issues

Using new media may present challenges with regard to intellectual property rights, such as government seals, copyright, and trademarks. OIGs should ensure that their external new media websites provide clear, concise statements about the intellectual property rights public users should be aware of. For example, an OIG might notify users that the government may not claim intellectual property rights in user-created content, but a third-party new media provider may, and users should check the third party's policy. Additionally, public-facing websites should warn users when use of government content might infringe on an intellectual property right.

Government Seals

In general, a private citizen may not upload an image of an agency seal or logo for use within a personal social media account. Government seals are not in the public domain.[229] Fraudulent, wrongful, or unauthorized use of a government seal or insignia

[229] A public domain work is a creative work that is not protected by copyright and which may be freely used by everyone.

is prohibited and punishable as a violation of the Federal criminal code.[230] Many agencies also have regulations that limit use of specific agency seals or insignia. For example, NARA regulations provide directions for authorized use of its seal or logo.[231] OIGs should make clear statements on their new media platforms indicating that use of the OIG seal is prohibited unless the user obtains written authorization from the OIG. It is important to protect against such improper use because the presence of an OIG's seal might give the appearance of an endorsement of the message or mission of a private person or entity.[232]

Copyrights

Owners of copyright protection enjoy the exclusive right to reproduce and distribute copies of their original works.[233] The copyright protections relevant to new media exist for original works of authorship in literary, musical, pictorial, graphic, motion picture, audiovisual, and sound recording works.[234] New media may raise several copyright issues, such as government ownership of copyrights, potential government infringement upon a private citizen's copyright, and copyrights available on third-party platforms.

OIGs should keep a few things in mind. First, copyright protection is not available for a U.S. Government work,[235] which includes any "work prepared by an officer or employee of the United States government as part of that person's official duties."[236] Accordingly, when an OIG employee creates and disseminates information through new media for official purposes, that information enters the public domain and cannot be subject to copyright protection by the employee or the OIG.[237] Government website content is owned by the government, not individual creators, and is likely to be agency record material.[238]

Second, although government works are not entitled to copyright protection, the government may obtain copyrights from private citizens by "assignment, bequest, or

[230] 18 U.S.C. § 1017 (wrongful use of government seals); 18 U.S.C. § 506 (knowing use of forged or counterfeit government seal); 18 U.S.C. § 701 (unauthorized manufacture, sale, or possession of a government insignia).
[231] 36 C.F.R. Part 1200.
[232] *See supra* Ethics section regarding endorsements.
[233] 17 U.S.C. § 106.
[234] *Id*. at § 102.
[235] *Id*. at § 105.
[236] *Id*. at § 101.
[237] See *Copyright and Other Rights Pertaining to U.S. Government Works*, USA.GOV, http://www.usa.gov/copyright.shtml for information on some exceptions to this general rule. For example, other people may have rights in the work itself or in how the work is used, such as publicity or privacy rights. Works prepared for the U.S. Government by independent contractors may be protected by copyright. Not all information that appears on U.S. Government websites is considered to be a U.S. Government work.
[238] *See Implications for Recent Web Technologies for NARA Web Guidance*, NAT'L ARCHIVES & RECORDS ADMIN., http://www.archives.gov/records-mgmt/initiatives/web-tech.html (last visited Aug. 16, 2013).

otherwise."[239] In addition, Federal employees may secure copyright protection for works written "at that person's own volition and outside his or her duties, even though the subject matter involves Government work or professional field of the official or employee."[240] For example, an OIG employee who drafts a white paper analyzing the impact of a piece of legislation as directed by her supervisor and then posts the paper on the OIG's social media websites cannot obtain copyright protection for that work. However, if the employee wrote an op-ed on the same piece of legislation and posted it on her personal social media website, she could secure a copyright for the work so long as the work was not required, and she wrote it on her own time. She could also choose to assign her personal copyright to the OIG.

Finally, an OIG cannot authorize an individual's use of copyrighted materials found on OIG websites hosted by third-party platforms. OIGs should consider adding disclaimer language similar to that of OGE's, which states that it "cannot authorize the use of copyrighted materials contained in linked websites."[241]

Liability for Copyright Infringement

OIGs may be liable for copyright infringement when using new media if they reproduce, distribute, or display a copyrighted work without the express permission of the author or copyright holder.[242] To establish a claim of copyright infringement, the copyright holder need only establish "ownership of the copyright . . . and copying by the defendant."[243] However, the "fair use" defense allows "people other than the copyright owner to use the copyrighted material in a reasonable manner without his consent."[244] Use of a work for "criticism, comment, news reporting, teaching, scholarship, or research does not infringe upon copyright."[245] Accordingly, OIGs may be able to use copyrighted material in new media forums without infringing on copyrights, so long as their use qualifies as a "fair use."

Courts consider four factors in determining whether the use of a work is fair:

- the purpose and character of the use, including whether the use is of a commercial or nonprofit nature;
- the nature of the work;

[239] 17 U.S.C. § 105.
[240] H.R. REP. NO. 94-1476, 58-59, *reprinted in* 1976 U.S.C.C.A.N. 5659, 5671-73 (1976).
[241] *See* OGE Disclaimer of Liability, *supra* note 110.
[242] *See* 17 U.S.C. § 106 (stating "the owner of copyright under this title has the exclusive rights to do and to authorize" the reproduction, distribution, and display or copyrighted works).
[243] Hustler Magazine Inc. v. Moral Majority Inc., 796 F.2d 1148, 1151 (9th Cir. 1986).
[244] *Id.*; *see also* 17 U.S.C. §§ 106, 107.
[245] 17 U.S.C. § 107.

- the amount and substantiality of the portion used in relation to the work as a whole; and
- the effect of the use on the potential market for or value of the work.[246]

Determining whether an OIG's use of a copyrighted work is fair requires a case-by-case analysis. The most important factor for OIGs to consider is whether a use of another's work might impair the marketability or the value of the copyrighted work.[247]

OIGs can protect themselves from copyright infringement liability by providing disclaimers on external-facing new media websites. For example, OIGs might post notices warning members of the public not to violate another's copyright and disclaiming liability for third-party social media activities that violate a copyright.

Trademarks

A trademark is any "any word, name, symbol, or device or any combination thereof" to identify and distinguish goods from those manufactured or sold by others and to indicate their source.[248] In intellectual property discussions regarding social media, trademarks can refer to agency logos and mission statements that appear on social media platforms. An official OIG social media platform should have some indicators of the official OIG trademark, demonstrating to the public the authenticity of the information presented on that website. Private individuals may not use OG trademarks or logos on personal social media websites without permission.

Several pieces of legislation have been created in attempts to protect the use of trademarks. For example, the *Trademark Act of 1946*, as amended,[249] also known as the *Lanham Act*, protects the use of trademarks and creates civil liability for persons who engage in trademark infringement. Specifically, it prohibits "any person" from using "in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive," without consent of the registrant.[250] "Any person" includes the U.S. Government.[251] The *Anticybersquatting Consumer Protection Act* prohibits mimicking other trademarks by using confusingly similar names or images.[252] Neither of these acts prevents fair use of a trademark. Additionally, the Uniform

[246] *Id*. at § 107(1)-(4).
[247] Craig C. Carpenter, *Copyright Infringement and the Second Generation of Social Media: Why Pinterest Users Should Be Protected from Copyright Infringement by the Fair Use Defense*, 16 J. INTERNET L. 1, 17 (2013).
[248] 15 U.S.C. § 1127.
[249] 15 U.S.C. §§ 1051 et seq.
[250] 15 U.S.C. § 1114(1)(a).
[251] *Id*. at § 1114(1)(b).
[252] 15 U.S.C. § 1125(a).

Domain Name Dispute Resolution Policy provides a process for registering domain names.[253] The policy creates a venue for trademark owners to bring forth challenges in private administrative proceedings.

Certain laws are in place to protect the use of trademarks, but OIGs may not always know when their official logo or brand is being used on nonofficial social media websites. Technology has made it easy for an individual to simply copy and paste a logo onto a new website, which may provide false information or divert the public to inappropriate material. This is especially concerning for OIGs if they collect personal information from the public; imposter websites may use deceit to obtain private information from unaware individuals. To discover fake social media platforms, OIGs might consider designating an individual to do a routine Internet sweep to determine if fake social media accounts have been created in the agency's name. Watching out for inappropriate trademark use can stem negative activities that may injure an OIG's reputation or dilute its message.

Public Accessibility

One of the goals of new media should be to help fulfill an OIG's mission of outreach and public affairs by providing information to the public in meaningful ways. However, when using new media, OIGs must be sensitive to the discrimination issues that can arise with regard to public accessibility to government communications. OIGs should ensure that they take steps to comply with laws providing access to government information and services to non-native English speakers and the disabled.

Section 508 of the *Rehabilitation Act*

Section 508 of the *Rehabilitation Act*, as amended, was enacted to ensure that people with disabilities have other means to access Federal information found online.[254] The law applies to all Federal agencies developing or maintaining IT and electronic technology. Section 508 requires agencies to provide disabled Federal employees and members of the public "access to and use of information and data that is comparable to the access to and use of the information and data" that is available to those without disabilities.[255]

Absent undue burden, every OIG must ensure that its social media communications provide equal access to individuals with disabilities.[256] One way to ensure Section 508

[253] *See Uniform Domain-Name Dispute-Resolution Policy*, ICANN, http://www.icann.org/en/help/dndr/udrp (last visited Aug. 16, 2013).
[254] 29 U.S.C. § 798.
[255] 29 U.S.C. § 794d(a)(1)(A).
[256] *Id.*

compliance is to create alternative methods of disseminating information and soliciting input to reach underrepresented groups. For example, OIGs can make sure that information posted on Twitter is also posted to their official websites, thereby providing those without Twitter accounts access to the same information. OIGs should ensure that their new media activities are "508 compliant" whether the content is on an internal or public-facing website, or includes software, websites, and services that are free.[257]

Accessibility for People with Limited English Proficiency

Executive Order 13166, *Improving Access to Services for Persons with Limited English Ability*, requires each Federal agency to ensure that people with limited English proficiency (LEP) have meaningful access to its services, programs, and activities so as to prevent discrimination on the basis of national origin.[258] The Federal Government has reinforced its obligations under this EO several times, most recently with a 2011 memorandum from the Attorney General.[259] Using social media and new media to interact with the public is agency activity that may require further steps to ensure that LEP individuals have meaningful access (i.e., translation into other languages).

To ensure that agencies provide meaningful access to LEP individuals, EO 13166 requires agencies to develop a plan. Department of Justice guidance establishes four factors to determine whether an agency needs to create and implement a plan to ensure meaningful access to LEP individuals: (1) the number or proportion of LEP individuals, (2) the frequency with which LEP individuals came in contact with an agency's programs, (3) the importance of the service provided by the program, and (4) resources available.[260]

Since the use of social media and/or new media would constitute an agency activity, the OIG must determine its LEP responsibilities. For assistance and guidance the OIG can consult its agency's LEP plan, contact its agency's LEP office, and refer to the Department of Justice guidance and other resources at www.lep.gov.

---

[257] *See Making Multimedia Section 508 Compliant and Accessible*, GEN. SERV. ADMIN., http://www.howto.gov/web-content/accessibility/508-compliant-and-accessible-multimedia (last visited Aug. 16, 2013).
[258] Exec. Order No. 13,166, 65 Fed. Reg. 50121 (Aug. 16, 2000).
[259] Eric. Holder, Jr., *Federal Government's Renewed Commitment to Language Access Obligations Under Executive Order 13166*, OFF. OF THE ATTORNEY GEN., U.S. DEP'T OF JUSTICE (Feb. 17, 2011), available at http://www.justice.gov/crt/lep/13166/AG_021711_EO_13166_Memo_to_Agencies_with_Supplement.pdf.
[260] Enforcement of Title VI of the Civil Rights Act of 1964—National Origin Discrimination Against Person With Limited English Proficiency; Policy Guidance, 65 Fed. Reg. 50123, 50124 (Aug. 16, 2000).

Liability

Along with all the legal and privacy issues comes a concern about potential liability. Indeed, torts litigation involving social media is a growing phenomenon. Defamation claims involving Twitter posts even have a name: "twibel" suits. However, while both OIG employers and employees may be liable for issues relating to social media activity, the risks at this point appear minimal. Nonetheless, an OIG should keep potential liability issues in mind while developing a social media policy and implementing social media for official purposes.

The FTCA constitutes a limited waiver of sovereign immunity, requiring any claim for money damages resulting from an employee's negligence or omission to be filed against the United States, as long as the employee was acting within the scope of employment.[261] Under the FTCA, the United States is liable if a private person would be liable in accordance with the law of the place where the act or omission occurred (absent any exclusions under the FTCA).[262] As a result, courts apply state law to determine whether an employee was within the scope of employment.[263] If an employee is found to be acting within the scope of employment, the employee is immune from all resulting suits.[264]

Although the FTCA does not completely waive sovereign immunity, Federal agencies are immune from certain torts, such as libel, slander, misrepresentation, and deceit.[265] In other words, if an employee, acting within the scope of employment, is sued for defamation for official OIG social media activity, the United States will substitute itself as a defendant, and neither the employee nor the OIG will be liable.

One tort that potentially could cause an OIG employer liability involves privacy, such as an invasion of privacy claim.[266] Each state may develop its own privacy laws, so the elements may vary state by state. In general, modern tort law has four generally recognized categories of invasion of privacy: intrusion of seclusion or solitude, public

[261] 28 U.S.C. § 2671, et seq.
[262] 28 U.S.C. §§ 1346(b)(1), 2674.
[263] Garcia v. United States, 62 F.3d 126, 127 (5th Cir. 1995) ("[W]hether a particular federal employee was or was not acting within the scope of his employment is controlled by the law of the state in which the negligent or wrongful conduct occurred").
[264] Note that the Westfall Act requires the Attorney General to certify that the employee was within the scope of employment. *See* 28 U.S.C. § 2679(d)(1)-(3). However, that determination may be challenged. *See* Gutierrez De Martinez v. Lamagno, 515 U.S. 417, 430-31 (1995) ("The certification, removal, and substitution provisions of the Westfall Act . . . work together to assure that, when scope of employment is in controversy, that matter, key to the application of the FTCA, may be resolved in federal court. To that end, the Act specifically allows employees whose certification requests have been denied by the Attorney General, to contest the denial in court.").
[265] 28 U.S.C. § 2680(h).
[266] *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960); RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977).

discourse of private facts, false light, and appropriation of a person's name or likeness.[267]

In addition, a citizen may sue the government for abridging his or her First Amendment (or other constitutional) rights. An employee acting within the scope of employment may be sued personally for a constitutional tort in a case often called a "Bivens" action.[268] However, the doctrine of qualified immunity allows government officials to exercise fair judgment and "provides ample protection to all but the plainly incompetent or those who knowingly violate the law."[269] This doctrine likely would protect an employee sued for deleting a member of the public's communications (an alleged violation of free speech rights), unless the employee willfully violated the law.[270]

With so many legal and privacy issues to consider, including potential liability, an OIG may hesitate before starting or expanding a social media program. The potential pitfalls demand not only knowledge at the outset, but also regular and continual maintenance. Despite potential pitfalls, however, OIGs will benefit from addressing the issues if only to steer employees in the right direction. No matter the degree to which an OIG engages new media, it can be sure that many employees already have an active social media presence.

In addition to the considerations discussed above, an OIG also needs to be aware of information security requirements. This next section will cover such information security issues as the *Federal Information Security Management Act of 2002*, cloud computing, social media, engaging new media providers, and protecting OIG networks.

Information Security Considerations

Social media services and new media often appear to confound the traditional security model for Federal agencies. Traditionally, agencies have controlled all aspects of an information system or contracted information services. Increasingly, however, as many social media services and new media apps are free, they can be provisioned outside of the authority of an agency's Chief Information Officer (CIO). In the past, the CIO has been primarily responsible through the *Clinger-Cohen Act of 1996*, as amended, for ensuring sound IT investments through associated laws, regulations, and Federal

[267] RESTATEMENT (SECOND) OF TORTS § 652E, cmt. b (2012).
[268] Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971) (Federal officials may be sued personally for money damages for the alleged violation of constitutional rights stemming from official acts).
[269] Malley v. Briggs, 475 U.S. 335, 341 (1986).
[270] Harlow v. Fitzgerald, 457 U.S. 800, 815 (1982) (holding that immunity would be defeated if an official "knew or reasonably should have known that the action he took within his sphere of official responsibility would violate the constitutional rights of the [plaintiff], or if he took the action with the malicious intention to cause a deprivation of constitutional rights or other injury . . .") (citing Wood v. Strickland, 420 U.S. 308, 322 (1975)).

policies. One of the key provisions of the *Federal Information Security Management Act of 2002* (FISMA), as amended, is to provide for the development and maintenance of minimum controls required to protect Federal information and information systems used by or on behalf of agencies. In practice, though, more attention has been given to the latter, as most Federal data resides on internal agency information systems that are tangible, traceable agency assets.

As OIGs embrace social media, the cloud, and other third-party websites and apps, Federal data will no longer receive the protections or assurance of fully assessed and accredited government networks, systems or personnel. In this new paradigm, data regularly traverses government and corporate networks, as well as domestic and international boundaries, where it is subject to varying degrees of protection.

As Federal data is stored, processed, and transmitted through unknown and often insecure environments, agencies expose themselves to new security and privacy concerns that they will need to address to ensure that they achieve success with these new tools and accomplish the agency's mission. Demand for social media and new media websites, apps, and services also puts pressure on OIGs to permit access to these websites, services, and apps through secure government networks.

The popularity of social media and new media websites, combined with their large memberships, make them attractive targets for malicious activities. When an OIG decides to allow access to these websites and services through secure government networks, additional safeguards and risk acceptance or mitigation need to be considered. OIGs will need to ask a few questions when proceeding with new media and the use of third-party storage. Where will the government data be hosted (internally, externally, hybrid)? Will the platform be used for internal or external communications, or both? The answer to these questions will have implications on which security laws, policies, and guidelines OIGs will need to follow.

Federal Information Security Management Act of 2002

FISMA was passed as Title III of the *E-Government Act of 2002* in December 2002. It requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[271] FISMA applies to all cloud computing, new media, and social media that stores, processes, or transmits Federal information. However, the application and implementation of FISMA-related

[271] *FISMA Frequently Asked Questions*, NAT'L INST. OF STANDARDS & TECH. (May 16, 2012), available at http://csrc.nist.gov/groups/SMA/fisma/faqs.html.

information security requirements to specific new media technologies may differ across OIGs based upon the types of information and how the technology is used in the various systems and services.

Pursuant to FISMA, OMB and the National Institute of Standards and Technology (NIST) issued standards and guidelines for how an agency should account for different information and information systems. These FISMA-related standards vary depending on the risk associated with the information and the information system. For example, agency use of public social media sites for public outreach may be considered low-risk, and a basic periodic risk assessment and implementation of some controls, including employee training, might be sufficient. In contrast, use of an internal information-sharing platform that contains sensitive agency information is higher risk and may involve more complex requirements, including comprehensive continuous monitoring.

Cloud Computing

Cloud computing is often the engine that drives new media tools and services. NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, apps, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[272] This applies to several service models including SaaS, Platform as a Service, and Infrastructure as a Service regardless of whether the hosting service is provided by another Federal entity or commercial organization. Cloud computing is also inclusive of services used for internal communications or external engagements such as social media.

To address the security implications of cloud computing, OMB released a memorandum titled *Security Authorization of Information Systems in Cloud Computing Environments* on December 8, 2011.[273] This memorandum formally sets the requirements created under the Federal Risk and Authorization Management Program (FedRAMP) as mandatory for Federal departments and agencies. FedRAMP establishes standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels that map back to FISMA requirements. It applies to executive departments and agencies procuring commercial and noncommercial cloud services that are provided by information systems that support the operations and assets of the departments and agencies, including systems provided or managed by other departments or agencies, contractors, or other sources.

[272] *The Definition of Cloud Computing*, NAT'L INST. OF STANDARDS & TECH. (Sept. 2011), available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
[273] Steven VanRoekel, *Security Authorization of Information Systems in Cloud Computing Environments*, OFF. MGMT. & BUDGET (Dec. 8, 2011), available at https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf.

The FedRAMP requirements are being phased in through June 2014. By that date, all Federal cloud instances are required to be in compliance with FedRAMP policy. Organizations will be required to self-identify and report annually to OMB the cloud services being used that do not meet FedRAMP requirements. In the meantime, departments and agencies are required to do the following:

- Leverage the FedRAMP process and security authorization requirements as a baseline when initiating, reviewing, granting, and revoking security authorizations for cloud services;

- Require cloud service providers to meet FedRAMP requirements in contractual provisions; and

- Assess, authorize, and continuously monitor security controls that are the agency's responsibilities.

The FedRAMP website, www.FedRAMP.gov, provides information on how to comply with the program's security requirements and guidance and how to structure standard contracting language for cloud service providers.

Social Media

The umbrella of new media also covers a range of social media tools, websites, and apps. On June 28, 2011, GAO released a report titled *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, which found that:

> most agencies did not have documented assessments of the security risks that social media can pose to federal information or systems in alignment with FISMA requirements, which could result in the loss of sensitive information or unauthorized access to critical systems supporting the operations of the federal government. Without conducting and documenting a risk assessment, agency officials cannot ensure that appropriate controls and mitigation measures are in place to address potentially heightened threats associated with social media, such as spear phishing and social engineering.[274]

Additionally, some of these services, apps or websites are third-party websites and apps that may be considered cloud computing-based SaaS subject to the requirements of FedRAMP. The FedRAMP program is still in its infancy, and most social media services

[274] *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605, GOV'T ACCOUNTABILITY OFFICE (June 2011), *available at* http://www.gao.gov/assets/330/320244.pdf.

will not have formal authorization packages on file with the FedRAMP program office in the foreseeable future. However, the security controls and guidance put forth by the FedRAMP office will help OIGs assess the security of social media services and formally authorize their use.

Engaging New Media Providers

When engaging in new media and social media services, OIGs are confronted with a significant risk-management challenge. In many cases, the service providers are willing to enter into a specific TOS with an OIG, during which time the OIG has an opportunity to negotiate as many security and privacy requirements as possible. At times, such negotiations will not be favorable to the OIG, and the OIG will be pressured to accept terms as provided by the new media or social media company. The following sections describe different tactics that OIGs may use to meet security and privacy requirements. OIGs should carefully review their relationship with social media and new media providers to ensure appropriate security and privacy matters are defined. OIGs should work with the new media providers to assess the security controls available and encourage the use of the available security controls in an effort to meet the Federal guidelines. Such topics include records retention, back-up of information, and securely storing credentials. Additional information may be found in appendix C.

Protecting OIG Networks While Accessing New Media Platforms

Consideration must be given as to when an OIG decides to have an official presence on a social media or new media platform, and equal consideration must be given as to how OIG users will access social media and new media services and websites. Many organizations and businesses block social media and new media websites for a variety of reasons, including security, privacy, and network performance. In crafting a new media or social media strategy, an OIG must also be aware of additional security and privacy challenges. Numerous technologies can aid an organization considering allowing access to new media and social media services and websites. OIGs should carefully consider which technologies may be appropriate to ensure secure access to social media and new media websites. They should address new media just as they would an internal system or network. Although the OIG does not own the new media, certain precautions should be taken before creating a presence on a new media website. For instance, OIGs should conduct a PIA and determine whether the application requires a SORN per the *Privacy Act*. The OIG should develop a Concept of Operations to formally authorize new media services and address how those services are leveraged and used. OIGs should conduct and provide training to those authorized to use new media. Training can provide guidance on recognizing operation security violations, limiting potential PII data breaches, promoting ethical behavior, and delivering appropriate information via new media. Additional information may be found in appendix D.

Conclusion

We encourage OIGs to consider using new media to further their mission, but as this report illustrates, new media has the potential to open many legal, privacy, and information security concerns. Even if an OIG declines to engage new media, it is prudent to develop appropriate policies and train employees in proper social media use. Missteps and problems may result from inadequate education and preparation.

Before embarking on a social media program, an OIG might consider analyzing its business need for social media based on such cost-benefit analysis questions as: Do we have the resources to start and maintain a social media program? Are we able to devote adequate personnel and resources to support and monitor an interactive blog or another social media network? How will those resources improve outreach and allow interactive communications with our stakeholders and the public? If we do not engage social media today, will we be behind tomorrow? Reaching out to other OIGs already engaged in new media may boost an OIG's confidence in its abilities to manage the legal, privacy, and information security issues.

On the information security front, OIGs preparing to deploy new media may discover that many of the required risk-management policies, procedures, standards, and guidelines are already in place. In IT planning, OIGs should include their CIO, Chief Information Security Officer, and Senior Official for Privacy. This will decrease potential legal, reputational, and monetary risks of using social media and new media services. OIGs also should consider whether investments in IT systems and software may be necessary to ensure proper risk mitigation.

As an OIG decides the extent to which it wishes to engage new media, we hope that this report will help facilitate informed decisions. However, this report should not be used as a substitute for independent legal advice, and the CIGIE New Media Working Group members and sponsors expressly disclaim liability for errors and omissions in the contents of this report.

Appendix A
Objectives, Scope and Methodology

We undertook this review at the request of CIGIE's Homeland Security Roundtable. The purpose of this review was to share new media legal, privacy, and information security research and analysis with OIGs. This analysis is designed to better equip OIGs that are engaging or starting to engage new media and, for OIGs not planning on using new media, to illustrate why being aware of the issues and developing a policy and training are nonetheless important.

The Working Group was staffed with attorneys and information security professionals from offices of presidentially appointed and designated Federal entity Inspectors General. The group met regularly from September 2012 until the spring of 2013. The Working Group conducted independent research and analysis, aided by the work of the original working group and consultations with specialists from NARA, the Air Force, the Federal Trade Commission, and GSA.

This report should not be used as a substitute for independent legal advice. New media is a fluid area, and laws and policies may change at a rapid pace. The CIGIE New Media Working Group members and sponsors expressly disclaim liability for errors and omissions in the contents of this report. No warranty of any kind, implied, expressed, or statutory, is given with respect to the contents. The information appearing in this report is for general informational purposes only and is not intended to provide legal, privacy, or information security-related advice to any individual or entity.

Appendix B
Sample New Media FISMA Legal Analysis

This appendix addresses the question of whether FISMA requirements (44 U.S.C. Sec. 3541, et seq.) apply to information that an OIG disseminates to the public using new media or social media. Messages are sent through new media and social media websites by establishing an account and sending messages through the Internet via the new media or social media website or mobile apps. FISMA requirements apply to new media and social media to the extent that these platforms are used to convey OIG information.

44 U.S.C. § 3541 sets forth the purposes of FISMA, which include providing effective government oversight over information security risks and maintaining minimum security controls required to protect Federal information and information systems. In furtherance of these goals, FISMA imposes requirements and responsibilities on OMB and on Federal agencies that relate to the establishment of programs to protect Federal information:

> *(a) In General. -- The head of each agency shall --*
> *(1) be responsible for --*
> *(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of --*
> *(i) information collected or maintained by or on behalf of the agency; and*
> *(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. . . .*[275]

In addition, FISMA states that each agency must establish an agency-wide information security program that includes, among other things, "periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency," and which ensures compliance with applicable standards promulgated under Section 11331 of Title 40 (the NIST standards).[276]

These provisions would encompass an OIG's use of new media and social media to communicate with the public because the information conveyed would be "information conveyed or maintained. . . on behalf of the agency," and the new media or social media system itself would qualify as an "information system used or operated . . . on behalf of an

[275] 44 U.S.C. § 3544(a)(1).
[276] *Id.* at § 3544(b).

agency." FISMA does not explicitly define the information to be protected and, consequently, also does not explicitly exclude OIG information conveyed via new media or social media from the information that must be secured through an OIG's required information security program. "Information systems" is defined as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."[277] This definition would include new media and social media as an information system, because OIG would use new media and social media as an information resource to share or disseminate information. Consequently, an OIG is obligated under 44 U.S.C. § 3544 to incorporate into its information security program the information conveyed via new media or social media and the information system itself.

OMB's computer security and FISMA guidance confirms this conclusion. OMB promulgated Circular A-130 to instruct agencies on how to implement information security requirements under earlier computer security statutes. Although A-130 pre-dates FISMA, its requirements are still applicable. In paragraph (a)(g) under "8. Policy," the Circular states that agencies must "[p]rotect government information commensurate with the risk and magnitude of harm that can result from the loss, misuse, or unauthorized access to or modification of such information. . . ." The Circular defines "government information" as "information created, collected, processed, disseminated, or disposed of by or for the Federal Government," which would include an OIG's social media and new media information. Under the question "How will agencies ensure security in information systems," OMB replies, "Apply OMB policies and . . . NIST guidance to achieve adequate security commensurate with the level of risk and magnitude of harm. . . ." OMB defines "information system" as "a discrete set of information resources organized for the collection, processing, transmission, and dissemination of information ... whether automated or manual." "Dissemination" is defined as "the government initiated distribution of information to the public." Because (1) OIG new media and social media information meets the definition of "government information," (2) new media and social media satisfies the plain meaning of "information system," and (3) the act of "posting" OIG information qualifies as "dissemination," there is no basis to exclude use of social media and new media from these requirements absent further clarification from OMB.

Pursuant to its FISMA obligations, OMB also promulgates annual FISMA reporting instructions. The 2010 instructions appear to require that new media and social media be used consistent with security requirements. FAQ 8 asks, "Should all of my agency's information systems be included as part of our FISMA report?" OMB answers, "Yes" (with further elaboration, but no limitation). As stated above, a new media and social media service qualifies as an "information system." In FAQ 11, OMB states that NIST standards must be applied to all non-national security information systems. In FAQ 13, OMB states, "Section 3541 of FISMA provides [that FISMA's] security requirements apply to 'information and information systems' without distinguishing by form or format; therefore, the security requirements outlined in FISMA apply

[277] 44 U.S.C. § 3502(8).

to Federal information in all forms and formats (including electronic, paper, audio, etc.)." In FAQ 25, OMB states that "security authorizations are required for all Federal information systems." In FAQ 36, OMB states, "[A]gency information security programs apply to all organizations (sources) which possess or use Federal information—or which operate, use, or have access to Federal information systems (whether automated or manual)—on behalf of a Federal agency."

Although the 2010 instructions do not specifically address use of social media or new media, FAQ 22 states that agencies should include SaaS and "software subscription" solutions in their annual security reviews. In conclusion, FISMA and OMB require that the standards be applied.

Appendix C
FISMA, NIST, OMB, FedRAMP, and Privacy Considerations

Federal Information Security Management Act

FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

GAO made the following statement in *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*:

> *The Federal Information Security Management Act of 2002 (FISMA) established a framework designed to ensure the effectiveness of security controls over information resources that support federal operations and assets. According to FISMA, each agency is responsible for, among other things, providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.*
>
> *Consistent with its statutory responsibilities under FISMA, in August 2009 the National Institute of Standards and Technology (NIST) issued an update to its guidance on recommended security controls for federal information systems and organizations. The NIST guidance directs agencies to select and specify security controls for information systems based on an assessment of the risk to organizational operations and assets, individuals, other organizations, and the nation associated with operation of those systems. According to the guidance, the use of a risk-based approach is applicable not just to the operation of the agency's internal systems but is also important when an agency is using technology for which its ability to establish security controls may be limited, such as when using a third-party social media service.*[278]

To meet FISMA compliance, social media and new media must have a risk assessment performed through compliance with the NIST risk management framework. The level of diffusion, use, and ease of provisioning of new media and social media makes it important to involve all business, technical, and legal stakeholders before engaging in social media to identify risks and where possible mitigate unnecessary risks. When determining FISMA applicability, it

[278] *Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605, GOV'T ACCOUNTABILITY OFFICE (June 28, 2011), *available at* http://www.gao.gov/assets/330/320244.pdf.

is important to engage counsel early in the process so they may understand the use of the technology, such as what types of information are being used and how the technology or service is being used on behalf of the OIG's mission.

The following sections address areas of information assurance and security as defined by NIST in fulfilling its statutory FISMA responsibilities. Should counsel determine that FISMA does not apply, the principles enumerated in the NIST Risk Management Framework should still be considered as they are industry best practices, which when implemented properly can greatly protect the OIG's data and reputation, and the public from fraud, waste, and abuse.

Federal Information Processing Standards Series

The Federal Information Processing Standards (FIPS) are NIST standards for computer information systems when there are compelling Federal government requirements, such as for security and interoperability. FIPS requirements are mandated by FISMA for the protection of Federal information and information systems. FIPS are thoroughly vetted by government and industry experts and often are voluntarily adopted by industry as best practices for enterprise security. FIPS represent the cornerstones of Federal information assurance and security. The following publications are the foundation of many Federal security programs:

- FIPS 140-2, *Security Requirements for Cryptographic Modules*;
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*; and
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems.*

If FISMA applies to the new media or social media application being used, then all applicable FIPS must be applied as appropriate. Minimally, however, FIPS 199 and FIPS 200 will apply to all services, systems, or apps. In many cases, a reasonable assurance of FIPS implementation and compliance for a new media or social media application will not be available as the OIG has little to no control of the platform. In these cases, the organization's authorizing official must weigh the possible violation of FIPS (and possibly FISMA) in light of overarching critical mission need and make a utilization or authorization decision.

NIST Special Publication 800 Series

The NIST Special Publication (SP) 800 Series was established in 1990 to provide an array of computer security research and guideline documentation relevant to IT practitioners. The series is the result of research and collaborative activities with industry, government, and academic organizations. While much of the series is considered to be general guidelines, SP 800-53, or *Recommended Security Controls for Federal Information Systems and Organizations*, is legally mandated for Federal agencies under FISMA through FIPS 200. The most recent version, Rev4, includes specific security controls related to planning (PL), access control (AC),

and Audit/Accountability (AU) for social media needs. Other relevant special publications for social media and new media include—

- SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*;
- SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*;
- SP 800-144, *DRAFT Guidelines on Security and Privacy in Public Cloud Computing*; and
- SP 800-145, *DRAFT A NIST Definition of Cloud Computing.*

These guides can help guide an organization through the NIST risk management framework. As the framework is applied to social media, new media, and cloud-based apps or services, a residual risk posture will be developed and give the organizational risk function a more informed environment to base decisions. The Chief Information Security Officer, Information Systems Security Officer, or Senior Agency Information Security Officer is typically well-versed in these documents, processes, and procedures. If an OIG employs IT auditors experienced in FISMA, FIPS, and the NIST SP 800 series, consider including them in any evaluation of new media or social media.

Office of Management and Budget Memoranda and Circulars

OMB issues executive orders, instructions, and guidance for Federal agencies in a variety of operational areas including security and privacy. In June 2010, OMB issued memoranda that provide specific guidance for the use of third-party websites and apps as well as the web measurement and customization technologies:

- OMB M-10-22*, Guidance for Online Use of Web Measurement and Customization Technologies*; and
- OMB M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications.*

M-10-22 and M-10-23 focus on privacy; the following memoranda and circular address security:

- OMB M-7-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*;
- OMB M-10-15, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; and
- OMB A-130, *Management of Federal Information Resources.*

Specifically, social media, or SaaS providers, are not inherently “Major Information Systems” as described by OMB Circular A-130, but they do qualify as “information systems” defined by 44 U.S.C. § 3502, since they are “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

Additionally, OMB M-10-15 states that all information systems, including SaaS, should be incorporated in an OIG's annual FISMA report. Further instructions in M-10-15 require agencies to perform security assessments for all information systems regardless of impact or use. Consider engaging the agency Chief Information Security Officer or Senior Official for Privacy when reviewing OMB security and privacy requirements.

Reporting (OMB/Departmental/Congress)

A vital component of all IT programs is the maintenance of an accurate, timely, and thorough inventory of all systems, software, and components. When systems and services are addressed under FISMA, they will be captured by an OIGs' annual reporting, and stand as a record of the system and a formal documentation of security controls for OIG information assets. When systems and services are not addressed under FISMA, there may be alternative reporting requirements to an OIG to catalog the use of third-party services.

Measuring and Managing Risk

Social media and new media services provide easy and accessible tools to communicate rapidly with a wide audience. This enhanced communication ability comes at the cost of increased risk. Risks range from threats to the confidentiality, integrity, and availability of data provided by the OIG to loss of reputation through public embarrassment if the OIG's account is compromised. These risks can be managed, accepted, or mitigated through specific and defined configurations and uses of social media and new media tools. For example, by requiring strong passwords and regularly changing them, or restricting the configurations of the tools and what types of information are processed, stored, or transmitted, an OIG can greatly reduce its risk posture. It is important to have a thorough understanding of all features and functions of the tools to be used and then document the desired use and configurations in conjunction with the information security or assurance function in an organization. Furthermore, it is important to understand what information the OIG is going to share or store from the service, as many social media tools provide access to large amounts of PII, and storing and accessing it can have *Privacy Act* implications.

Continuous Monitoring

Unlike traditional continuous monitoring approaches for Federal information systems, social media systems are not in the total control of the OIG. Despite this limitation, continuous monitoring can be conducted in a limited and usually manual fashion. Specifically, OIGs should monitor their social media services as continuously and as near real-time as possible to ensure that their accounts have not been modified or that unofficial information has not been posted to their account. This can be accomplished through documenting changes to the website and storing backups of that data on internal OIG systems. Additionally, the technology behind social media is constantly evolving as new features and functionality are rotated into the

service offerings. It is important that OIGs maintain their awareness and stay up-to-date of changes regarding the products that they use. Some new media and social media services will make sweeping and drastic changes to the controls that protect information. These changes could come from new features or additional privacy settings that must be taken into account. For this reason, it is important for OIGs to regularly reevaluate the risk of the use of these tools. This should also occur with any major content releases or updates to the social media service. PIAs and security assessments should be routinely reviewed when a significant change occurs and on a time-based schedule to ensure they are still accurate, thorough, and timely. For more information about continuous monitoring, review the following publications:

- NIST FAQ on Continuous Monitoring; and
  NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*.[279]

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a collaboration among NIST, the GSA, the Department of Defense, DHS, the CIO Council, state and local governments, the private sector, nongovernmental organizations, academia, and working bodies such as the Information Security and Identity Management Committee. FedRAMP's goal is to develop an innovative policy approach to developing trusted relationships between Federal Executive departments and agencies and cloud service providers.

[279] *Frequently Asked Questions: Continuous Monitoring*, NAT'L INST. OF STANDARDS & TECH. (June 1, 2010), available at http://csrc.nist.gov/groups/SMA/fisma/documents/faq-continuous-monitoring.pdf.

Appendix D

Negotiating, Contracting, and Communicating Information Security Requirements

Engaging New Media Providers

When engaging in new media and social media services, OIGs are confronted with a significant risk management challenge. In many cases, the service providers are willing to enter into a specific TOS with an OIG, during which time the OIG has an opportunity to negotiate as many security and privacy requirements as possible. At times, such negotiations will not be favorable to an OIG, and the OIG will be pressured to accept the terms provided by the new media or social media company. The following sections describe different tactics that an OIG may employ in trying to meet security and privacy requirements.

Voluntarily Meet Federal Information Security Requirements

For some social media and new media services, security can be considered an afterthought, if not counterproductive, to engaging and growing a user base. However, many established providers are compelled to maintain their customer base by improving service and security in parallel. In recent years, the Federal Trade Commission has cited several social media providers for misleading consumers about their level of privacy protection and information security practices. Settlement agreements with the providers have required audits by independent third parties. Audit results can be used to help understand the information security risks involved in using platforms. Some social media services have already begun using ISO 27001/2 and FISMA-compliant security programs and are willing to share their progress with Federal agencies. When researching social media tools, due diligence should be performed to reach out to the companies and engage in security and privacy dialogue so that the OIG's risk management function is able to develop a comprehensive understanding of the risk it may be exposed to while using the service.

Contractual Options for Information Assurance

Social media services are generally free tools available for personal and enterprise use. However, some service providers offer variations of a tiered service, such as free and paid subscription models. In addition to enhanced user features in some of the paid subscriptions, there are often enhanced security configurations as well. When reviewing a social media service that offers a tiered service plan, it is advisable to enquire about the security configuration differences between the tiers to be able to make an informed decision before employing one of these tools. Additionally, a paid service model gives the OIG an opportunity to negotiate a contract with the service provider and add security and reporting requirements.

Always ensure that a contracting officer and counsel are involved in these activities since legal and contracting issues do arise.

FedRAMP Standard Contract Language

FedRAMP has developed a security contract clause template to assist Federal agencies in procuring cloud-based services. This template should be reviewed by an OIG counsel to ensure that it meets all requirements, and then incorporated into the security assessment section of a solicitation. The template covers FedRAMP requirements for areas like the security assessment process and related ongoing assessment and authorization. The template also provides basic security requirements identifying cloud service provider responsibilities for privacy and security, protection of government data, personnel background screening, and security deliverables with associated frequencies.

Appendix E

Protecting OIG Networks While Accessing New Media Platforms

Great consideration must be given when an OIG decides to have an official presence on a social media or new media platform, and equal consideration must be given as to how users will access social media and new media services and websites. Many organizations and businesses block social media and new media websites for a variety of reasons including security, privacy, and network performance. In crafting a new media or social media strategy, the OIG must also be aware of additional security and privacy challenges. Numerous technologies can aid an organization that is considering allowing access to new media and social media services and websites.

Web Proxy and Web Filters

Web filters and proxies are designed to filter and block malicious, illegal, inappropriate, or unwanted web content. Many agencies employ web filters to block designated pages; however, they also often block social media and new media websites because of the amount of malware and malicious content potentially distributed by these tools. OIGs employing only web filters often rely on separate Internet connections through aircards, digital subscriber lines, or similar technologies. Web proxies are typically much more expensive and require greater management, but also allow for much greater flexibility in allowing access to websites by simulating a computer and then opening the content on it first and observing the behavior using a variety of antivirus and antimalware tools. If the content is deemed acceptable according to the defined risk threshold, it is passed on to the end user. If the content is deemed malicious, the end user is informed that the content they are trying to access has been quarantined. CIOs and information system security officers can provide more information about web proxies and filters. If an OIG is planning to allow access to new media or social media websites, it should strongly consider implementing a web proxy. A web proxy will not protect against all malicious attacks but will greatly reduce the risk of accessing social media and new media websites.

Data Loss Prevention and Protection

Data loss prevention (DLP) tools are used to examine the types of information leaving an OIG's network. As social media and new media typically offer the ability to post large amounts of information on the service, OIGs must be able to detect sensitive information exfiltration. Many DLP tools can be configured to detect PII, credit card numbers, phrases, and specific combinations of information. Many of these tools can also be configured to detect sensitive information in compressed files, documents, and common office documents. DLP tools are typically a considerable investment and require management support and operational overhead to operate successfully.

Secure Workstations or Terminals

Even with web proxies, DLP, and other security controls, OIGs must exercise defense when deciding to allow users to access social media or new media services. Most agencies are required to adhere to the Federal Desktop Core Configuration or the U.S. Government Configuration Baseline when purchasing desktops, laptops, and servers. These configurations harden and strengthen the overall security posture of workstations that may access new media or social media services. Consider using the concept of "least privilege" for user accounts when determining the depth and breadth of workstation-hardening activities. An example of "least privilege" could be ensuring that all workstations and end-user devices use "restricted" or "limited" accounts by default. These accounts allow the common commands that a standard user needs to work while restricting the use of commands that could damage a system. Only users such as helpdesk and system administrators would be issued accounts that could harm the system if used incorrectly, such as with "administrative" or "root" level accounts.

Security Operations Centers and Continuous Monitoring

DLP, web proxies, and other technologies are limited by the reaction time of an OIG to a malicious attack or event. When deciding to allow access to social media or new media websites, the OIG should consider if a security operations center should be employed, or if already employed, if additional tuning of the security operations center's functions will be required. In the event that a center is not employed, the OIG should evaluate its continuous monitoring program for its general support system and ensure that it is providing reporting in as near real-time as possible to the organization's risk management function.

Appendix F
Major Contributors to This Report

The CIGIE New Media Working Group

The CIGIE New Media Working Group consisted of representatives of the following Offices of the Inspectors General:

- Department of Agriculture
- Department of Defense
- Department of Health and Human Services
- Department of Homeland Security
- Department of Housing and Urban Development
- Department of the Interior
- Environmental Protection Agency
- Legal Services Corporation
- National Science Foundation
- Pension Benefit Guaranty Corporation
- Social Security Administration
- Treasury Inspector General for Tax Administration
- United States Postal Service

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.