



**Homeland
Security**

**DHS 4300A
Sensitive Systems Handbook**

**Attachment X
Social Media**

**Version 14
July 24, 2018**

Document Change History

Version	Date	Description
0.6	March 25, 2010	Final Draft for Comment
0.7	May 12, 2011	Final Draft for Review; Includes Component Comments
8.0	May 23, 2011	Final
9.1	July 24, 2012	Stylistic and formatting changes throughout the document
11.0	August 5, 2014	Additional stylistic changes throughout.
14.0	July 24, 2018	Thoroughly revised to conform to current standards and best practices. Thoroughly updated with regard to Privacy issues. Version numbered to coincide with current 4300A Policy edition (No version 11, 12, nor 13 of this Attachment was published).

Contents

1.0	Introduction	1
1.1	<i>Background</i>	1
1.2	<i>Purpose and Scope</i>	2
1.3	<i>Application</i>	2
2.0	Use of Social Media	3
2.1	<i>Official Public Affairs Use of Social Media</i>	3
2.1.1	<i>Governance</i>	3
2.1.2	<i>Privacy Issues</i>	3
2.1.3	<i>Standards of Conduct</i>	4
2.2	<i>Operational Use of Social Media</i>	5
2.2.1	<i>Authority</i>	5
2.2.2	<i>Privacy Compliance Documentation</i>	5
2.2.3	<i>Access</i>	6
2.2.4	<i>Rules of Behavior</i>	6
2.2.5	<i>Privacy Training</i>	7
2.2.6	<i>Retention of PII</i>	7
2.3	<i>Unofficial or Personal Use of Social Media on Government Equipment</i>	7
2.4	<i>Unofficial or Personal Use of Social Media on Non-Government Equipment</i>	7
3.0	Risks and Attack Techniques Associated with Social Media	9
3.1	<i>Common Risks of Cyber Attacks</i>	9
3.2	<i>Common Cyber Attack Techniques</i>	10
3.2.1	<i>Spear Phishing</i>	10
3.2.2	<i>Social Engineering</i>	10
3.2.3	<i>Web Application Attacks</i>	11
4.0	Best Practices for Social Media Use	12
4.1	<i>Personal Use of Social Media</i>	12
4.2	<i>Never Post Classified or Sensitive Information</i>	12
4.3	<i>Never Speak for the Department without Authorization</i>	12
4.4	<i>Avoid Posting Personal Information</i>	12
4.5	<i>Use Privacy and Security Settings</i>	12
4.6	<i>Be Wary of Location-Based Services</i>	13
4.7	<i>Use Strong Passwords</i>	13
4.8	<i>Be Suspicious about Installing Applications</i>	14
4.9	<i>Be Wary of All Links</i>	14
4.10	<i>Have No Expectation of Privacy</i>	14
4.11	<i>Protect Your Privacy</i>	15
4.12	<i>Be Professional</i>	15
4.13	<i>Use Disclaimers</i>	15
4.14	<i>Be the First to Respond to Your Own Mistakes</i>	15
4.15	<i>Be Yourself</i>	15
4.16	<i>Avoid Being Offensive</i>	16
4.17	<i>Do Not Breach Trademarks</i>	16
4.18	<i>Respect Copyright, Fair Use, and Financial Disclosure Laws</i>	16
4.19	<i>If in Doubt, Seek Guidance</i>	16
5.0	Unofficial Internet Posting Guidelines	17

Glossary..... 19
References..... 25

.

1.0 INTRODUCTION

Social media such as Facebook, Twitter, and Instagram have become ubiquitous in our daily life. According to a study by the Pew Research Center, nearly two-thirds (65%) of all American adults use social network sites—a nearly tenfold jump in the past decade¹. Due to extensive casual Internet use, it comes as no surprise that Federal employees and contractors may have difficulty deciding what constitutes acceptable and security-conscious behavior in using social media.

Even as Government organizations consider how best to leverage the interactivity enabled by social media, they must also ensure a common understanding of how employees are expected to use those media.

Issued under the authority of the Department of Homeland Security (DHS) Chief Information Officer (CIO), through the Office of the Chief Information Security Officer (OCISO), this document expands on existing DHS policy as provided in Section 3.16, “Social Media,” of *DHS Sensitive Systems Policy Directive 4300A*, and in DHS Management Directive (MD) 4400.1, “Web (Internet, Intranet, and Extranet Information) and Information Systems.”

This document is applicable under the following guidelines:

- Whether or not the use is official (work-related) or unofficial (personal)
- Whether or not the use occurs on sanctioned “official” social media sites or on commercially managed sites
- Whether or not use is accomplished using Government-issued equipment or on electronic devices owned by the employee or other third-party.

1.1 Background

Cyber attacks on and via social media are rapidly increasing because of the abundance of personal information available on social media sites that is of interest to cybercriminals such as home address, family names, friends’ names, and current employer. Due to the high threat of **malware** infiltration and the sensitive nature of the information maintained at DHS, social media host sites are blocked at the Department’s Trusted Internet Connections (TIC).² The Assistant Secretary, Office of Public Affairs (OPA), as well as Component public or external affairs offices, however, do permit limited social media use “by exception,” through sanctioned Government and commercial social media sites and social networking services. These limited uses of social media make information and services more widely available. Sanctioned social media can:

- Provide additional sources that the public can use to obtain supplemental information about the Department’s activities

¹ “Social Media Usage: 2005-2015”, Pew Research Center, October 6, 2016, <http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/>

² Section 3.16, *DHS Sensitive Systems Policy Directive 4300A*.

- Provide opportunities for participation and collaboration on Department activities
- Reach a wider audience more efficiently through the use of social media capabilities
- Showcase the Department’s work and integration
- Support Department and Component missions

Unofficial (personal) social media usage can easily make DHS personnel and the Department victims of *social engineering* or other forms of cyber-attack. Employees need guidance to help minimize the risks their social media use poses to the Department and its missions.

1.2 Purpose and Scope

This document provides guidance regarding official (work-related) and unofficial (personal) social media use whether occurring within or outside the Department network, the risks and attack techniques associated with social media, and best practices for social media use.

1.3 Application

This document applies to all DHS Federal employees and contractors, describes the governance of social media sites across DHS, and addresses the use and associated risks of social media technologies in three scenarios:

- Required work-related use
- Unofficial or personal use on Government equipment
- Unofficial or personal use on non-Government equipment

The term *equipment* includes both non-portable devices such as desktop computers as well as mobile devices such as laptop computers smartphones and tablets.

Commonly used social media terms are in bold italics throughout this attachment and are defined in the Glossary.

2.0 USE OF SOCIAL MEDIA

2.1 Official Public Affairs Use of Social Media

Many Federal Departments and agencies are required to publish Government information for public engagement or external affairs purposes. Component offices of public or external affairs publish materials on dhs.gov, which is the official website and presence of DHS. In addition, some Components maintain their own websites, subject to departmental oversight.

Instructions for using dhs.gov and commercial or third party social media are provided at the DHS Web Center (see www.dhs.gov/webcenter).

As a result of these technological relationships between the Department and the public, it is imperative that DHS engage the public in a manner that complies with Federal accessibility, privacy, information security, and records requirements.

2.1.1 Governance

The DHS Office of Public Affairs (OPA) serves as the primary account holder for all DHS and Component social media websites, approves and manages all content posted, and when necessary acts as the final authority on comment acceptability. OPA will ensure that posted content meets the requirements for publicly available information and materials.

2.1.2 Privacy Issues

To protect Personally Identifiable Information (PII) internally and when engaging the public, DHS employees must comply with Federal privacy laws, Office of Management and Budget (OMB) guidance, and DHS privacy policies when using social media in an official capacity. The Privacy Office is responsible for ensuring that DHS use of social media sustains and does not erode privacy protections concerning the use, collection, and disclosure of *PII*.

It is imperative that the Department be transparent about its use of social media to avoid concerns about unauthorized surveillance. Therefore, DHS must engage social media websites in a manner that protects privacy and respects users' intent. The public user fully expects privacy protections while interacting with the Department. In order to address these and other concerns, the DHS Privacy Office has set forth specific requirements for using social media in a privacy- sensitive manner.

Each social media website provides its own privacy policy, and while users are typically required to submit some PII during the registration process, the Department will neither solicit nor collect such PII. The Department will examine the social media website or application privacy policy and evaluate the risks to determine whether or not the website is appropriate for the Department's use. If an agency posts a link that leads to a social media website, the agency will provide an alert to the visitor, either a statement adjacent to the link or a "pop-up," explaining that visitors are being directed to a non-government website that may have different privacy policies from those of the agency's official website.

The Department will only collect the minimum information necessary for the performance of official functions. Official DHS accounts on social media websites will be identified by the Department or Component seal and an easily identifiable account user name indicating DHS presence, such as "DHS Jane Q. Employee."

As part of the Department’s privacy compliance process, the DHS Privacy Office has developed two Department-wide Privacy Impact Assessments (PIA), both found at www.dhs.gov/privacy, to identify and mitigate privacy risks for the Department’s use of social media for public engagement or external affairs:

- “Use of Social Networking Interactions and Applications (Communications/Outreach/Public Dialogue),” September 16, 2010
- “Use of Unidirectional Social Media Applications,” March 8, 2011

These two PIAs and the DHS privacy policies, including those that are social media specific, govern the Department’s use of social media from a privacy standpoint. The DHS privacy policy as well as privacy policies specific to social media can be found at www.dhs.gov.

PIA determination is made on a case by case basis through the social media privacy threshold analysis (SMPTA). Components should work with their Component Privacy Office to ensure compliance with privacy requirements. DHS Headquarters should contact the DHS Privacy Office directly at (b)(7)(E)

Approved PIAs are published on the Department’s Privacy Impact Assessment Web page (see www.dhs.gov/topic/privacy) unless they are classified. DHS has issued a PIA detailing the PII to which the Department may have access because of its use of social networking applications, how it will use the information, what information is retained and shared, and how individuals can gain access to and correct their information.

If PII is posted on a social media site, the Department will attempt to delete it. If that is not possible, the Department will disregard the PII and it will not be maintained in agency files. It should be noted, however, that PII posted on a social media website or sent to the Department in connection with the transaction of public business may become part of a Federal record and will have to be maintained in accordance with appropriate records retention policies.

Note that this privacy compliance framework does not apply to the Department’s “operational use of social media.” See section 2.2 for details.

2.1.3 Standards of Conduct

DHS employees and contractors are responsible for knowing and following the guidelines in DHS Directive) 262-04, “DHS Web (Internet and Extranet Information)” (Revision 00) and Executive Branch conduct guidelines, such as “Standards of Ethical Conduct for Employees of the Executive Branch,” when using social media in an official capacity. These standards cover topics of prohibited activities such as:

- Engaging in vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups
- Endorsement of commercial products, services, or entities
- Endorsement of political parties, candidates, or groups
- Lobbying members of Congress using DHS or any other appropriated resource
- Use of Government resources to foster commercial interests or individual profit

Federal employees often inadvertently fail to comply with the stringent requirements of the Hatch Act of 1939, which governs political speech by Federal employees. The U.S. Office of Special Counsel (OSC) issued “Hatch Act Social Media and Email Guidance” regarding the applicability of the Hatch Act to social media engagement in the workplace by Federal employees³. The Hatch Act’s restrictions may determine whether or not Federal employees are allowed to post content that could be interpreted in a political light. Employees should understand the Hatch Act, and Sections 4 and 5 of this document, before posting on social media or revealing professional titles or political affiliations.

2.2 Operational Use of Social Media

As part of the Department’s homeland security missions, DHS personnel may engage in the operational use social media to meet their mission requirements, consistent with their existing authorities and subject to the approval of the Chief Privacy Officer.

Pursuant to the DHS Management Directive 110-01, “Privacy Policy for Operational Use of Social Media” (June 8, 2012), “operational use” means the authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings.

2.2.1 Authority

Program Managers and System Managers must consult with counsel to ensure that appropriate authority exists to engage in categories of operational use of social media before Component employees engage in those activities.

2.2.2 Privacy Compliance Documentation

Before engaging in, or contracting for, new or modified categories of operational use of social media (which as defined includes investigatory purposes), Program Managers and System Managers, in consultation with Component Privacy Officers or Privacy Points Of Contact and counsel must complete a Social Media Operational Use Template (SMOUT) to document the authority and purpose(s) of those uses as well as a description of those uses, and to determine whether all of the Rules of Behavior discussed below will apply to the particular uses(s) covered by the SMOUT.

Please contact the DHS Privacy Office at (b)(7)(E) for a blank SMOUT form.

SMOUTs are submitted to the Chief Privacy Officer for a prompt review and determination as to whether a new or updated PIA or SORN is required. SMOUTs are also completed to document

³ Official of Special Counsel, “Hatch Act Social Media and Email Guidance”, <https://osc.gov/Pages/Hatch-Act-Social-Media-and-Email-Guidance.aspx>

categories of operational use of social media in existence prior to this Instruction to ensure compliance with this Instruction. Once a SMOUT is approved for a category of operational use, a new SMOUT is not required for additional use of social media within that category unless there is a material modification of the Rules of Behavior applicable to that category. Components may appeal to the Deputy Secretary of Homeland Security if there is a disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

2.2.3 Access

DHS employees who are authorized to use social media by their Component heads renew their access authority annually, consistent with annual training requirements. Access is contingent upon an employee's successfully completing privacy training for operational use of social media.

2.2.4 Rules of Behavior

Component Privacy Officers or PPOCs, in coordination with counsel and Program Managers, or System Managers as appropriate, draft Rules of Behavior for operational use of social media (either separately or as part of a broader policy document) and submit them with the Template to the Chief Privacy Officer for review and approval. Personnel granted access to use social media certify annually that they have read and understand the Component Rules of Behavior. Where certification is not practicable, Component Privacy Officers and PPOCs maintain records of employee attendance at privacy training that includes training on Rules of Behavior.

Rules of Behavior must include requirements for operational use of social media and the consequences of failure to adhere to those requirements. Where a federal policy establishes guidelines that apply to a Component's operational use of social media, the Component's Rules of Behavior incorporate that policy and that fact is noted in the Template.

Unless otherwise noted in the Template adjudication process, the Rules of Behavior provide, at a minimum, that DHS employees:

1. Use social media for operational purposes only when activities are authorized by statute, executive order, regulation, or policy.
2. Use only government-issued equipment, government accounts, and only government email addresses when engaging in the operational use of social media.
3. Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties.
4. Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information.
5. Respect individuals' privacy settings and access only information that is publicly available unless the individual whose information the employee seeks to access has given consent to access it.
6. Collect the minimum PII necessary for the proper performance of their authorized duties;
7. Protect PII as required by the Privacy Act and DHS privacy policy.

8. Document operational use of social media, including date, site(s) accessed, information collected, and how it was used in the same manner that the Department would document information collected from any source in the normal course of business. For instance, where information obtained through authorized operational use of social media is used in whole or in part to make decisions regarding an individual's rights, benefits or privileges, employees document that fact in relevant records.
9. When use of the social media site is completed, always log out of the site.

2.2.5 Privacy Training

Component Privacy Officers or PPOCs tailor privacy training for the operational use of social media to Component-specific needs, based upon training materials provided by the Chief Privacy Officer. Completion of this privacy training is a prerequisite for obtaining access to social media for operational use. Upon completion of this training, employees will certify that they have read and understand their Component's Rules of Behavior. Where certification is not practicable, Component Privacy Officers and PPOCs maintain records of employee attendance at privacy training that includes training on Rules of Behavior. Employees also complete refresher training and recertify they have read and understand their Component's Rules of Behavior annually thereafter. Privacy training content includes, at a minimum, legal authorities, acceptable operational uses of social media, access requirements, applicable Rules of Behavior, and requirements for documenting operational uses of social media.

2.2.6 Retention of PII

Component Program Managers or System Managers where appropriate, maintain PII collected through authorized operational uses of social media in the applicable Privacy Act system of records in accordance with approved records retention schedules.

2.3 Unofficial or Personal Use of Social Media on Government Equipment

Social media is an attack vector routinely exploited by cybercriminals, whose activities may expose the Department to unacceptable risk. Additionally, social network activity consumes bandwidth and can negatively impact employee productivity. DHS prohibits personal access to social media from Government equipment unless an exception to policy has been granted.

Although DHS employees are authorized limited personal use of DHS office equipment in accordance with DHS Management Directive (MD) No. 4600.1, "Personal Use of Government Office Equipment," such authorization does not apply to the use of DHS equipment for personal use of social media. This restriction also applies to contractors and other individuals using DHS equipment.

2.4 Unofficial or Personal Use of Social Media on Non-Government Equipment

Employee activities potentially affect DHS job performance, the performance of others, and DHS business interests. Any information posted on the Internet incurs a level of risk, because that information is exposed indefinitely with no reliable methods for deletion or retraction. In addition, because of the connected nature of the Internet, even information presumed to be posted in a venue with restricted access is potentially accessible to anyone.

“Unofficial Internet posts” result when DHS personnel express DHS-related thoughts, ideas, knowledge, experience, and opinions on any Internet site, whether or not the site is DHS-controlled. Unofficial Internet posts are personal expressions developed and released by an employee or contractor that have not been initiated by any official part of the DHS organization or reviewed through an official DHS approval process. Employees must remember that any information about another individual is almost surely protected by the Privacy Act and should not be shared.

Social networks are of particular concern because of the potential for users to disseminate personal information about themselves and others. Unless strict privacy controls are applied to online profiles, the information posted is viewable by a wide range of strangers. Normally adversaries would have to engage in determined information gathering in order to collect sensitive information, but social networks can easily provide them an opportunity to gather sensitive information with relative ease. Even seemingly harmless facts can be collected and used by adversaries to assemble profiles and select targets. Even with privacy controls in place, DHS employees and contractors should not post any content that they would not be comfortable disclosing to the public.

Employees must remember that any information that is work-related is sensitive and cannot be repeated outside the workplace without appropriate approval. In addition, further limits are in place if you identify yourself, whether directly or indirectly, as a DHS employee.

Consistent with the risks detailed above, the recent guidance issued by the U.S. Office of Special Counsel (OSC) regarding social media outside the workplace does not differ substantially from guidance for the workplace, although more latitude is given for employees to express political thoughts and candidate advocacy and support on their personal websites. See Sections 4 and 5 of this document for additional best practices and guidelines applicable to social media use.

3.0 RISKS AND ATTACK TECHNIQUES ASSOCIATED WITH SOCIAL MEDIA

Adversaries look for opportunities to easily target persons of interest on the Internet in order to develop footholds for long-term surveillance and exploitation. Social media sites are attractive to hackers since the same technologies that invite user participation make user systems easy to corrupt with *malware* such as *worms* that can shut down networks, *spyware*, or *keystroke loggers* that can steal sensitive data. For example, the availability of *widgits* makes it easier for social networkers to share links, insert pictures, etc., but it also makes it easier for an attacker to slip in malicious code or to link to off-site content that contains *malware*.

3.1 Common Risks of Cyber Attacks

The risks associated with social networking fall into a few broad categories:

- Accidentally releasing sensitive information
- Hackers gaining information through a social networking site that will allow the hacker to attack the *enterprise network*
- Having the social networking account itself hacked
- Identity theft
- Users picking up *malware* through the social networking site

Government use of social media also poses potential privacy risks. Social media users voluntarily provide PII in their user profiles (examples are hometown and employer), making such information available to other registered users, including DHS. The availability of this PII does not give the Department the authority or right to collect, use, or disclose that information absent a separate authority to do so.

The emergence of *Location-Based Services (LBS)* (geo-location) poses additional privacy concerns. Research undertaken by Carnegie Mellon University in 2009 and 2010⁴ found that “currently available location-sharing services do not, for the most part, do a good job of informing [users] about how their location information will be used or provide users with expressive location privacy controls and privacy-protective default settings.” Furthermore, although Section 222(f) of the Communications Act⁵ generally prohibits wireless carriers from using location-based information for commercial purposes without the express prior consent of the consumer, these prohibitions do not currently apply to LBS providers even though their applications are being downloaded on the devices of wireless carriers.

Consumers may mistakenly conclude that application providers are subject to the same prohibitions as wireless carriers and that no action by consumers is necessary to ensure that their

⁴ “Location-Sharing Technologies: Privacy Risks and Controls”, Carnegie Mellon University, February 1010, http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf

⁵ “Communications Act of 1934”, Federal Communications Commission, <https://transition.fcc.gov/Reports/1934new.pdf>

privacy is protected.⁶ The DHS Privacy Office requires all projects, programs, or systems contemplating the use of LBS to submit a PTA.

3.2 Common Cyber Attack Techniques

According to the *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*⁷, social media technologies such as *wikis*, *blogs*, and *social networks* are especially vulnerable to the following cyber-attack techniques:

- Spear phishing
- Social engineering
- Web application attacks

3.2.1 Spear Phishing

Spear phishing is an attack targeting a specific user or group of users, attempting to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current issues. Sometimes this information is gathered by hacking into the targeted network, but often it is easier to look up the target on a social media network.

In April 2009, the Federal Bureau of Investigation (FBI) released a Headline Alert citing social networking sites as a mechanism for attackers to gather information on their targets by harvesting information from publically accessible networks and using the information as an attack vector⁸. Spear phishers use social media as an alternative way to send phishing messages, as the social media platform bypasses traditional email security controls. Security teams have already observed multiple social media websites used as a propagation mechanism to trick users into opening a document or clicking a link. DHS daily receives many specific attacks via email targeting specific employees by name and position.

3.2.2 Social Engineering

The second concern regarding social media use by Federal employees is **social engineering**, which relies on exploiting the human tendency to trust. The attacker's first step in any social engineering attack is to collect information about the target. Social networking websites can reveal many details of personal information, including resumes, home addresses, phone numbers, employment information, work locations, family members, education, and photos. Social media websites may share more personal information than users expect, need, or realize. For example, a study by the University of Virginia cites that out of the top 150 Facebook applications, all of which are externally hosted, over 90% needed nothing more than publicly available information

⁶ Joint Hearing on "The Collection and Use of Location Information for Commercial Purposes", February 24, 2010.

⁷ "Guidelines for Secure Use of Social Media by Federal Departments and Agencies," Version 1.0, Federal CIO Council, September 2009.

⁸ "Spear Phishers: Angling to Steal Your Financial Info", FBI, April 2009, https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109

from members in order to operate. In every case, however, users needlessly granted the applications total access to their account and therefore full access to all personal information.

When DHS employees join a social media website, they may identify themselves as DHS employees. Their self-identification creates a DHS *Internet footprint*, which is valuable information to adversaries. As more Federal employees self-identify on social media websites, the Federal footprint on social networking will grow, creating a target-rich environment to help adversaries target specific individuals to launch various social engineering attacks.

To learn personal information about an individual, an attacker can express a common interest in a topic and build a trust relationship with the victim. This positions the attacker to influence the victim's friends and co-workers or even to collect sufficient information to pose as the victim, providing an easy avenue for penetrating the trust of the Department or of other DHS personnel.

High-profile Federal employees with greater name recognition are an especially prime target for a social engineer seeking to exploit trust relationships in social networks.

3.2.3 Web Application Attacks

Malicious content on social networking sites is easy to disguise as valid content. Developers of user-generated games and applications on some sites have the option of going through an approval process, but the application's code is not always locked in the state in which it was submitted for approval. This creates a situation in which apparently vetted software can be injected with malicious code at a later time.

Finally, while a hijacked personal social media account may be annoying and personally costly or embarrassing, the hijacked account of a Federal user or a hijacked Federal account can have more serious implications. Unauthorized posts, tweets or messages may be seen by the public as official messages, or may be used to spread malware by encouraging users to click links or download malware and unwanted applications.

4.0 BEST PRACTICES FOR SOCIAL MEDIA USE

Online activities often blur the line between individuals' personal and professional lives. Real-world social and business rules have counterparts in digital environments. DHS employees or contractors, in or outside of the workplace, may affect their job performance, the performance of others, or DHS business interests, so they are a proper audience for best practice guidance. The following guidelines are intended to assist DHS employees and contractors in protecting their personal information and reputation while interacting online. These best practices are based on guidelines established by other Federal and commercial organizations.

4.1 Personal Use of Social Media

Use social media only on personal time using your personal computer and email account. You should not be logged onto external social networking sites while at work.

4.2 Never Post Classified or Sensitive Information

Posting classified or sensitive information on a social media site will lead to significant adverse action and penalties. DHS Management Directive No. 11042.1, "Safeguarding Sensitive But Unclassified (For Official use Only) Information" establishes DHS policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS, and other sensitive but unclassified information received by DHS from other Government and nongovernment activities. Do Not Communicate DHS Policies

4.3 Never Speak for the Department without Authorization

Never answer questions or make statements about or on behalf of DHS on a social networking site without explicit authorization from the DHS Office of Public Affairs, the DHS Office of General Counsel, or their Component equivalent.

4.4 Avoid Posting Personal Information

Limit the amount of personal information you post to social networks. Avoid posting personal information such as your home address, personal phone numbers, or details about your schedule or routine. This type of information gives cybercriminals the baseline they need for more targeted activities. Assume that anything you post to a social network can be seen by anyone and act accordingly. Also be wary of the type of information — including photographs — that you post about your friends and family, since that information can put them at risk.

4.5 Use Privacy and Security Settings

When accessing social networking sites, you can limit disclosure by using the site's Privacy settings. The default settings for some sites may allow anyone to see your profile. You can customize your settings to restrict access to only certain people. Also be aware of any changes to the site's privacy or security options. For example, Facebook is constantly improving user privacy settings that users should be aware of and implement as soon as possible⁹. Users should

⁹ "Facebook Privacy: 10 Settings to Check", Information Week, June 5, 2014, <http://www.informationweek.com/software/social/facebook-privacy-10-settings-to-check/d/d-id/1269438>

monitor the privacy policies for social networking sites as they change often and without warning. Remember though, there is a risk that even private information can be exposed, so do not post anything that you would not want the public to see.

4.6 Be Wary of Location-Based Services

Be aware of privacy and security issues when using location-based services (LBS). LBS offers many conveniences such as keeping track of family and friends, getting directions, finding restaurants, and assisting in law enforcement. But LBS may make information about your location accessible to unintended recipients. Employees should understand that use of LBS introduces significant privacy and personal security risks with their use. The most common example is using a location check-in service (for example, Foursquare). If you check in from your couch at home, the precise Global Positioning System (GPS) coordinates of your couch are published. If you later check in from your office, it can be seen that you are no longer at your home, which is now an excellent target, and your own personal security can be compromised.

Carefully consider any request by any application to allow use of your location or any other personal information. In Snapchat and in other applications that can show your location or that of your contacts, always use a “ghost” mode that disallows showing your location. You should also be aware that this information may leak unintentionally. For example, smartphones can attach GPS coordinates to pictures you take. Posts made to social media sites such as Facebook or Twitter may also contain this detailed geo-location data that could also compromise your personal security and possibly your workplace security. The location attached to the picture may be metadata that is uploaded without your knowledge.

Be sure to examine your phone’s privacy, security, and location settings to ensure that GPS coordinates are not automatically associated with LBS. Be sure never to check in from sensitive locations and avoid establishing patterns when possible.

4.7 Use Strong Passwords

Protect your account with passwords that cannot be easily guessed. Avoid using passwords such as your dog’s name, the word “password” plus a digit, or your favorite sports team name.

A strong password resists guessing. Hackers and computer intruders use automated software as a way to submit hundreds of guesses per minute to access your account. These software tools are called 'dictionary' or 'brute force repetition' tools, because they will use English dictionaries to sequentially guess your password. These password-guessing tools can submit up to 1000 attempts per minute. The less that your password resembles regular word patterns, the longer it will take for a repetition tool to guess it.

These password variations below purposely avoid using complete English word patterns. Passwords that use combinations of characters that include numerals, symbols, and capital letters as well as lower case letters will create an exponentially longer task for attackers using dictionary programs and brute force.

Do not use the same password for multiple applications.

Even strongly constructed passwords are vulnerable to keystroke loggers and password cracking tools. In the final analysis, passwords do little to deter a determined attacker.

According to NIST (National Institute of Standards and Technology), a strong password should contain no fewer than 12 characters, a rule adopted by the U.S. government in 2007 and further defined in the [U.S. Government Configuration Baseline](#). Admin passwords should be 15 characters. Readers may sigh at those lengths, but they have been the recommended minimum for half a decade. Anything shorter is not considered secure.

4.8 Be Suspicious about Installing Applications

Applications from social media sites are very often given complete access to your account—not just to what is necessary for the application to run. “Quizzes” are also problematic. For example, Facebook users taking quizzes can reveal far more personal information to the applications than they realize. This is mostly due to the fact that Facebook’s default privacy settings allow access to all your profile information whether or not your profile is set to “private.”

Even if you do not take quizzes yourself, your profile information may be revealed when one of your friends takes a social media or Internet quiz. Almost everything on your profile, even if you use privacy settings to limit access, is available to the quiz.

4.9 Be Wary of All Links

Vigilance is the best defense against phishing. Phishing scams can arrive in e-mails that look as though they come from real companies or trusted individuals. For example, you may receive an e-mail message announcing that your bank account will be closed unless you confirm your personal identification number, or that you need to provide your credit card information to confirm an order, or requesting verification of your social security number for billing purposes. Legitimate companies do not ask for your account or personal information via e-mail. To find out whether the message is legitimate, contact the company directly by telephone or letter using contact information from a trusted source, such as your account statements.

Never reply to suspect emails or click on any links they contain. This could expose you to clickjacking, in which a web page will trick you into performing undesired actions by clicking on concealed buttons or links that are on a web page hidden by the visible one. For example, the page may list what appears to be a valid DHS web page address, such as www.dhs.gov; however it hides the link to a web site set up by a cybercriminal. To find out whether the message is legitimate, contact the sending company directly by telephone or letter using data from a trusted source, such as your account statements or the back of your credit/debit card. Another way to verify the validity of the web page is, instead of clicking on an embedded link, manually enter the URL into the navigation bar of your web browser to avoid clickjacking.

Phishing attempts can also come in Twitter “tweets”, Facebook wall postings, videos, or pictures sent via email. Get into the habit of not clicking on hyperlinks, especially those for videos or news-related events from unfamiliar sources and senders. In many cases, these are linked to phishing and social engineering attacks.

4.10 Have No Expectation of Privacy

Assume that your thoughts are in the public domain. Remember that social networking sites are generally public and permanent, even if you delete the information you posted. You should understand the security and privacy features available for the social networking sites you use,

and exercise discretion and common sense. Most social networks offer settings to keep profiles private and restrict access to personal photographs or other personally identifiable details; however, opting for privacy does not guarantee that others will not see your content. Content can be forwarded or hacked.

Facebook has found itself at the center of privacy breakdown controversies numerous times, and confusing Twitter interfaces have resulted in private messages being inadvertently posted to public feeds. Hackers can force access and friends can forward your content to others. In short, do not post anything that you do not want the public to see.

4.11 Protect Your Privacy

Do not share personal or contact information about your family, friends, co-workers, clients, or businesses without their explicit consent. Do not post or tag pictures of family, friends, co-workers, clients, or business without their consent. Respect the privacy of others at all times. Always protect your PII.

4.12 Be Professional

If you identify yourself as a DHS employee or have a public-facing position so that your DHS association is known to the general public, ensure that your profile and related content are consistent with how you wish to present yourself as a DHS professional, even if the information is of a personal and unofficial nature. Ensure that all your posts and interactions are consistent with the public trust associated with your position, and conform to existing standards such as “Standards of Ethical Conduct for Employees of the Executive Branch.”

If you establish online profiles, you may provide your DHS title and contact information. You may also indicate that DHS is your employer, and you may describe your past and present job responsibilities (as you would on your resume) if you do not disclose any DHS sensitive information or the personal information of others.

4.13 Use Disclaimers

Be aware of your DHS association in online social networks. If your profile reveals your employment relationship with DHS, you should include a disclaimer stating that your activity and posts represent your personal opinions and do not represent those of DHS. An example of an appropriate disclaimer is “The postings on this site are my own and do not represent the positions, strategies, or opinions of the Department of Homeland Security.”

4.14 Be the First to Respond to Your Own Mistakes

If you make an error, be up front about your mistake and correct it quickly. In a blog, if you choose to modify an earlier post, make it clear that you have done so.

4.15 Be Yourself

Do not forge or manipulate identities in your posts in an attempt to disguise, impersonate, or misrepresent your identity or affiliation with any other person or entity.

4.16 Avoid Being Offensive

Do not post defamatory, libelous, vulgar, obscene, abusive, profane, threatening, racially and ethnically hateful, or otherwise offensive or illegal information or material.

4.17 Do Not Breach Trademarks

Do not use any word, logo, or other mark that would infringe on a trademark, service mark, certification mark, or other intellectual property rights of the owners of such marks without the permission of such owners.

4.18 Respect Copyright, Fair Use, and Financial Disclosure Laws

Do not post any information or other material protected by copyright without the permission of the copyright owner. Also, consider using a Creative Commons license to protect your own work. Creative Commons offers a flexible copyright model through a collection of free copyright licenses written in plain language. Creators can select several of these licenses to communicate which rights they reserve, and which they waive, when their intellectual property is used by others. Wikipedia is one of the most notable web-based projects using a Creative Commons license. See www.creativecommons.org for additional details.

4.19 If in Doubt, Seek Guidance

Seek guidance from the DHS Office of Public Affairs or the DHS Office of General Counsel, or Component equivalent, prior to publicly sharing any personal opinions or statements based on your role within DHS. Those with leadership responsibilities, by virtue of their position, especially must understand that personal thoughts they publish, even in clearly personal venues, inadvertently may be interpreted as expressions of official DHS positions. They should assume that their co-workers, employees, and those outside of DHS will read what they have written.

5.0 UNOFFICIAL INTERNET POSTING GUIDELINES¹⁰

Department of Homeland Security (DHS) personnel who post content about DHS on the Internet are responsible for ensuring that any information disclosed (including personal comments) is accurate and appropriate. DHS personnel should keep in mind how their posts will reflect upon themselves and their organization, and also be aware that some individuals and groups use public networking forums to gain information that will help them advance their own causes or agendas at the expense of others. DHS personnel who engage in unofficial posting on the Internet should observe the following guidelines:

- (1) You may not release DHS e-mail addresses, telephone numbers, or fax numbers not already publicly released. You may not release the content manager's or content provider's work contact information.
- (2) You may not post or disclose the existence of internal DHS documents or information that DHS has not officially released to the public. This policy applies no matter you obtained the information. Examples include, but are not limited to, the following: memos, e-mails, meeting notes, articles for publications, white papers, Public Affairs guidance, and all pre-decisional materials. Do not release any For Official Use Only (FOUO) information or PII in unofficial Internet posts.
- (3) You, as a DHS Federal employee or contractor, are always responsible for adhering to DHS policies concerning information security, physical security, and to the Privacy Act in all forms of communication. Unauthorized disclosure of protected information, including sensitive but unclassified (SBU) information may result in disciplinary action.
- (4) You may not release information about or pertaining to another DHS employee. Release of classified, operational, proprietary, law enforcement sensitive, or investigatory information is not authorized.
- (5) Any photo, video, or sound recording made by DHS personnel of an official DHS function is considered official DHS media. Newsworthy items should be released officially to news organizations and other media with the knowledge and approval of OPA or the Component office of public or external affairs before being posting unofficially.
- (6) DHS-related media made by DHS personnel while they are in a non-working status in public areas, (e.g., photo of a U.S. Coast Guard cutter taken from a public pier while on liberty) is considered private imagery and is not subject to these guidelines.
- (7) Use of official or protected DHS statements or symbols (for example, the DHS logo) must be approved OPA. This prevents the impression of official or implied endorsements.
- (8) You may not release, intentionally or unintentionally, location-based (geospatial) information related to a DHS mission. This prohibition includes, for example, disclosing the location of the employee and/or DHS assets at a particular point in time. **Auto-**

¹⁰ Based on US DHS, ALCOAST 548/08, COMDTNOTE 5700. SUBJ: SOCIAL MEDIA - UNOFFICIAL INTERNET POSTS.

tweeting, geospatial coordinates while driving, or reporting via a location-based social media tool such as ***Foursquare*** are examples of violations of this guideline.

- (9) As with other forums of personal public engagement, DHS personnel shall avoid off-duty behavior that negatively impacts, or conflicts with, their ability to execute their duties for DHS, such as the prohibited personal conduct described in Standards of Ethical Conduct for Employees of the Executive Branch.

GLOSSARY

Terms commonly used in relation to social media are defined below.

Term	Explanation
Blog	An abbreviation of “weblog.” A blog is a web-based forum where individual content providers contribute regular entries or “posts” in the form of commentary, descriptions of events, or other materials on the website. Visitors to the blog may add their own comments to posts. Blogs may be “moderated” with the blog owner overseeing removal of any objectionable material, or they may be “unmoderated,” in which case there is no control over the posted material.
Clickjacking	A malicious technique of tricking a user into revealing confidential information or of taking control of their computer when they click links on seemingly harmless web pages. On a clickjacked page, the attacker shows a set of dummy buttons or links, then loads another page over it in a transparent layer. Users think they are clicking on the visible page while they are actually performing actions on the hidden page which the users never intended, such as changing privacy settings on a social networking site or following someone on Twitter.
Commercial/Third Party Social Media	Social media hosted on servers over which DHS has no control. This includes proprietary social networking sites such as Facebook and MySpace, as well as collaboration services such as Wikipedia, BlogSpot, and Delicious.
Content Manager	Any individual designated to manage web content for DHS or a Component. The duties of the Web Content Manager include ensuring compliance with accessibility standards for persons with disabilities. This individual is the organization’s primary point of contact for Web issues. ¹¹
Content Provider	Any individual who creates content for publication to DHS websites. ¹²
Enterprise Network	The communications backbone that interconnects every computer and associated device at every location under the jurisdiction of an organization, such as DHS.
External Hosting	Provision by an external organization or company of access, on a fee-per-service basis, to the equipment, technology and support to needed to establish and run a website, as opposed to an organization’s using its own in-house resources.
Farming	See Pharming
Fishing	See Phishing

¹¹ DHS 4300A, IV Definitions, J

¹² DHS 4300A, IV Definitions, K

Term	Explanation
Foursquare	A location-based social networking website and application for mobile devices. Users “check in” or report their location by accessing a mobile website, text messaging or a device-specific application, so that their whereabouts can be discovered by others. Foursquare also incorporates elements of a game by awarding users points for being the first to visit a new place, and for adding new information about the locations they visit.
Hacker	A person who uses their proficiency with electronics, computers and/or programming skills to gain illegal access to others’ digital resources, including personal handheld devices, files, computers and networks.
Internet footprint	The collective activities and behaviors recorded as an individual interacts in a digital environment, including device usage, system logins and logouts, website visits, files, transmitted emails, and posted messages. “Passive footprints” are created when data are collected about individuals’ activities without any deliberate action on their part, such as tracking which products customers are visiting on a vendor’s website regardless of whether purchases occur. “Active footprints” are created when personal data is released intentionally by individuals for the purpose of sharing information with others online. Footprints are sometimes used as a rough measure of an individual’s “web presence.”
Keystroke loggers	Also called a “keylogger,” It is can be a hardware device or a program that monitors and records each keystroke a user types on a computing device’s keyboard. Although sometimes used for legitimate purposes, such as diagnostics or monitoring a child’s Internet activity, a more typical use of keystroke loggers is for the unauthorized capture of security credentials such as passwords and personal identification numbers.
Malware	Derived from the phrase “malicious software,” this term is a generic term for any program whose purpose is to cause harm to a computer system. Typically, malware is installed without the user’s knowledge or consent, although it is often packaged with other software the user does in fact choose to install or download. Viruses and worms are examples of malware.
Mashup	A web page or application that enables the fast, easy combination of data and/or functionality from multiple sources to create a new, enriched result that was not necessarily the reason for producing the original sources. Most mashups use publicly-accessible resources. For example, a mashup might superimpose on a Google map of a neighborhood the average housing prices drawn from a city assessor’s online database.
Metadata	Information about the meaning of other information. Metadata can describe or summarize key attributes of a piece of information to facilitate finding that information when needed. An example of metadata is a time stamp that specifies when a piece of information was created.
Micro-Blog	Extremely short blog posts similar to text messaging. The messages can either be viewed by anyone or by a restricted group that is chosen by the user. Twitter, a popular micro-blog client, allows posts of up to 140 characters to be uploaded and read using instant messaging or mobile devices via text messaging.

Term	Explanation
Operational Use	The authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual.
Password Attack	An attempt to obtain a legitimate user’s password. Hackers can use common password lists, dictionaries, cracking programs, and password sniffers in password attacks.
Personally Identifiable Information (PII)	Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the United States. Examples of PII include, but are not limited to name, date of birth, mailing address, telephone number, Social Security Number, email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), IP addresses, biometric identifiers (e.g., fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic), and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual. Also, Sensitive Personally Identifiable Information (SPII) that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual. ¹³
Pharming	An action whereby a hacker subverts a user’s attempt to visit a legitimate website by instead redirecting themr to a counterfeit or “spoofed” website. The spoofed site is designed to trick users into revealing personal information such as usernames, passwords, and account information.
Phishing	An attempt to fraudulently acquire a user’s personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Phishing is common in e-mail and instant messaging. For example, you might receive an e-mail that appears to come from an official at your bank that instructs you to “confirm” your Internet banking credential by clicking on a link. The “spoofed” website to which you would be directed would capture your credentials in order to enable a third party to access and withdraw all funds from your bank account.

¹³ DHS 4300A, IV Definitions, H

Term	Explanation
Sensitive Personally Identifiable Information (SPII)	Sensitive PII is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised. SPII includes Social Security Number, driver’s license or State ID number, passport number, Alien Registration Number, financial account number, and biometric identifiers.
Social Bookmarking	A Web-based service where users create and store links to information on topics of particular interest to them. Although web browsers have the ability to bookmark links to “favorite” pages, those links are tied to an individual browser on a single computer. Social bookmarking, by contrast, stores links in an online account which can be made public. These bookmarks can be shared and discovered by others who are interested in finding information on similar topics. Examples of social bookmarking sites include Delicious, Digg, and Reddit.
Social Engineering	The act of deceiving or tricking people into performing actions or divulging confidential information, rather than obtaining such information by breaking in or using technical means. For example, someone posing as a help desk representative might telephone you and claim to be diagnosing a connection problem; the caller requests that you verify your login ID and password or other personal information so it can be checked against the items on file.
Social Media	Internet-based applications that build on the foundations of Web 2.0 to allow the creation and exchange of user-generated content. Social media can take many different forms, including but not limited to Web-based communities and hosted services, social networking sites, video and photo sharing sites, wikis, blogs, podcasts, virtual worlds, social bookmarking, and many emergent technologies.
Social Networking Services	Web-based services that connect people who share the same interests and/or activities, or who are interested in exploring the interests and activities of others. Social networking services provide a variety of ways for users to interact. For example, Facebook is used as a place to socialize with friends, whereas LinkedIn caters to those who wish to make professional connections.
Spam	Unsolicited or undesired electronic messages. Spam includes legitimate advertisements, misleading advertisements, and phishing messages— any unsolicited message can be spam.
Spear Fishing	See Spear Phishing
Spear Phishing	A technique by which the attacker generates an e-mail message or prompts linking to a website. The attack’s target is a specific individual or small group. The goal is to convince the targets to take action, which gives the attacker access to their system by presenting them with text, images, or URLs that they could actually expect and therefore mistake for legitimate.

Term	Explanation
Spoofed Website	An impostor website that mimics a real company’s website in order to steal personal information from site visitors. Victims are often directed to these spoofed sites through phishing e-mails. Spoofed sites can look extremely convincing, but often contain small flaws such as spelling errors or “slightly wrong” logos.
Spyware	Any software that covertly gathers users’ information through their computing devices and/or their Internet connection without their knowledge for unauthorized use. Spyware applications are typically hidden components that users inadvertently download together with legitimate material. Spyware may gather information such as e-mail addresses for advertising purposes, or even passwords and credit card data.
Trusted Internet Connections (TIC)	A DHS initiative implementing OMB Memorandum M-08-05, to optimize and standardize the security of individual external network connections including connections to the Internet that are currently in use by the Federal Government. A “TIC” is a physical location an agency uses to meet the objectives of the TIC Initiative.
Twitter	A social networking micro-blogging service that enables its users to send and read other users’ messages, called “tweets.” Users (“followers”) may subscribe to (“follow”) other users’ tweets. Twitter is sometimes called the “Short Message Service of the Internet” because of the compatibility of its interface with smart phones. Tweets are limited to 140 characters.
Uniform Resource Locator (URL)	In computing, the identifier that specifies where a resource is located and the mechanism for retrieving it. The best-known example of the use of URLs is for the addresses of web pages on the Internet, such as www.dhs.gov .
Video Sharing	Websites on which users post video they have taken for others to view and comment on. Such sites allow viewers to “embed” or display others’ video on their own sites. YouTube is probably the most widely known video sharing site.
Virtual world	Online communities where users or their digital representations (called “avatars”) can socialize, connect, and interact with one another using text and voice chat. The term is used more specifically to refer to an online community such as Second Life that features a computer-based simulated three-dimensional environment where users can not only interact but also create and use virtual objects.
Virus	A form of malware that can copy itself and spread from one computer to another in the form of executable code when its host is taken to a target computer. For example, a user might send an infected file over a network, or carry it on a removable medium such as a CD or thumb drive, or the virus might send an instant message to all the contacts on the infected machine which, when opened by the addressee, infects the recipient’s computer. While some viruses are benign, often a virus will cause a computer to “hang,” rendering it inoperable by corrupting and/or disabling key operating system files and tools.

Term	Explanation
Web 2.0	Although there is no agreed-upon definition of the term <i>Web 2.0</i> , it term generally refers to the move toward a more social, interactive, collaborative, and responsible Web. It can be characterized by capabilities and tools facilitating social media dialog.
Whaling	Phishing attacks targeted at high-ranking personnel in an organizational hierarchy, such as Chief Executive Officers (CEO) and other top executives.
Widget	A self-contained tool that can be embedded in a website or program to deliver a single-purpose service, such as displaying the latest news and weather, maps, or photos, or allowing a user to play interactive games with other website visitors. Users of social networking sites often take advantage of widgets as an easy way to make their sites more interesting to visitors; care must be taken, however, since hackers often use widgets as malware entry points.
Wiki	A technology for creating collaborative websites. From the Hawaiian word meaning “quick,” a wiki is a collection of Web pages that encourages users to contribute or modify the content. By using a simple Web interface, a community can collaborate to develop a document or Web page, no matter where the members of the community are located. By far the best-known wiki is Wikipedia, a multilingual, web-based, free content encyclopedia project.
Worm	Self-replicating malware that uses a computer network to send copies of itself from one computer system to another. Worms can cause excessive network traffic and other malicious disruptions such as file deletion and sending junk mail to every e-mail address it discovers on every computer system as it spreads throughout a network.

REFERENCES

Federal Regulations

“Standards of Ethical Conduct for Employees of the Executive Branch,” 5 CFR 2635

DHS Directives)

Directive 110-01, “Privacy Policy for the Operational Use of Social Media,” June 8, 2012

MD No. 11042.1, “Safeguarding Sensitive But Unclassified (For Official Use Only) Information,” January 6, 2005

Directive 139-05, “Office of Accessible Systems and Technology,” January 29, 2016

MD 262-04, “DHS Web (Internet, and Extranet Information)” (Revision 00), April 13, 2015

MD 4600.1, “Personal Use of Government Office Equipment,” April 14, 2003

MD 4900, “Individual Use and Operation of DHS Information Systems/Computers,” undated DHS Privacy Office Publications

MD 110-01, “Privacy Policy for the Operational Use of Social Media,” June 8, 2012

Instruction 110-01-001, “Privacy Policy for Operational Use of Social Media,” June 8, 2012

DHS Privacy Office Publications

“DHS Privacy Impact Assessment for Use of Social Networking Interactions and Applications,” DHS Privacy Office, April 2010

“Government 2.0: Privacy and Best Practices: Report on the DHS Privacy Office Public Workshop, DHS Privacy Office, November 2009

Congressional Proceedings

Joint Hearing, “Collection and Use of Location Information for Commercial Purposes,” U.S. House of Representatives, Energy and Commerce Committee, Subcommittee on Communications, Technology and the Internet, and Subcommittee on Commerce, Trade, and Consumer Protection, February 24, 2010

Other Government Sources

“CIO Council Guidelines for Secure Use of Social Media by Federal Departments and Agencies,” Federal CIO Council, Version 1.0, September 2009

“Communications Act of 1934”, Federal Communications Commission, <https://transition.fcc.gov/Reports/1934new.pdf>

“GSA Social Media Policy and Handbook,” CIO 2106.1, General Services Administration, July 17, 2009

“Hatch Act Social Media and Email Guidance,” Office of Special Counsel, <https://osc.gov/Pages/Hatch-Act-Social-Media-and-Email-Guidance.aspx>

“New Media and the Air Force,” U.S. Air Force Public Affairs Agency, Emerging Technology Division, April 6, 2009

“Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions,” Federal Web Managers Council,” December 23, 2008

“Social Media Security Mitigations,” Version 1.1, U.S. Centers for Disease Control and Prevention, December 3, 2009

Articles and White Papers

“Security Threat Report: 2010,” Sophos Group, 2010

“The Application Usage and Risk Report: An Analysis of End User Application Trends in the Enterprise,” Palo Alto Networks, Fall 2009

“Location-based Social Media Has Legal Implications for Employers & Employees,”
www.thesocialworkplace.com, April 16, 2010

“Location-Sharing Technologies: Privacy Risks and Controls”, Carnegie Mellon University, February 1010,
http://cups.cs.cmu.edu/LBPrivacy/files/TsaiKelleyCranorSadeh_2009.pdf

“Spear Phishers: Angling to Steal Your Financial Info”, FBI, April 2009,
https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109