Guidelines for Secure Use of Social Media by Federal Departments and Agencies

Information Security and Identity Management Committee (ISIMC)
Network and Infrastructure Security Subcommittee (NISSC)
Web 2.0 Security Working Group (W20SWG)

Version 1.0

September 2009

This document is publicly releasable

Intended Audience

This document is intended as guidance for any federal agency that uses social media services to collaborate and communicate among employees, partners, other federal agencies, and the public.

Note: The Federal CIO Council does not endorse the use or imply preference for any vendor commercial products or services mentioned in this document.

TABLE OF CONTENTS

Revision History

Date	Revision	Description of Changes
5/15/09	0.1	Initial draft release
6/28/09	0.2	Major revision, including section changes, formatting changes, figures
7/14/09	0.3	Revisions for formatting, reordering, improving document flow
7/21/09	0.4	Revisions based on Web 2.0 Security Working Group (W20SWG) feedback.
8/7/09	0.5	Revisions based on Network and Infrastructure Security Subcommittee (NISSC) feedback
8/10/09	0.6	Initial comments from Federal CIO Council
8/30/09	0.7	Initial release through Federal CIO Council
9/7/09	0.8	Second release through Federal CIO Council
9/9/09	0.9	Final release through Federal CIO Council
9/14/09	1.0	Final Comments integrated

Acknowledgements

The Web 2.0 Security Working Group operates under the authority of the Information Security and Identity Management Committee (ISIMC), as chartered by the Federal CIO Council (FCIOC).

The Information Security and Identity Management Committee (ISIMC) is the principal interagency forum for identifying and recommending strategic high priority IT security and identity management initiatives to the FCIOC and Office of Management and Budget (OMB) that enable the Federal Government's information systems security programs and agencies' mission objectives.

The Web 2.0 Security Working Group (W20SWG) is a representative body responsible for assessing information security issues surrounding Web 2.0 technologies in the Federal Government, and recommending solutions to mitigate identified risks.

For the purposes of this working group, Web 2.0 includes social media and cloud computing. This working group will provide best practices and recommendations for federal use of social media and cloud computing resources.

Name	Role	Organization
Robert Carey	ISIMC Co-Chair	Department of the Navy
Vance Hitch	ISIMC Co-Chair	Department of Justice
Earl Crane	ISIMC NISSC W20SWG Chair Primary Author/Editor	Department of Homeland Security
Mark Brown	Reviewer/Contributor	Department of Health and Human Services
Brian Burns	ISIMC NISSC Co-Chair Reviewer/Contributor	Department of the Navy
Trisha Christian	Reviewer/Contributor	Small Business Administration
Christy Crimmins	Reviewer/Contributor	Department of the Navy
Eric Eskelsen	Reviewer/Contributor	Department of Education
Matt Fischer	Reviewer/Contributor	Transportation Security Administration
Peter Flynn	Reviewer/Contributor	Department of Veterans Affairs
Daniel Galik	Reviewer/Contributor	Department of Health and Human Services
William Gill	Reviewer/Contributor	Environmental Protection Agency
Nancy Kaplan	Reviewer/Contributor	National Science Foundation
Gregory Mann	Reviewer/Contributor	National Aeronautics and Space Administration
Mitra Nejad	Reviewer/Contributor	Department of Justice
Dr. Julie Ryan	Reviewer/Contributor	The George Washington University
Steve Ressler	Reviewer/Contributor	Department of Homeland Security
Edward Roback	Reviewer/Contributor	Department of Justice
Roger Seeholzer	Reviewer/Contributor	Department of Homeland Security
Michael J. Smith	Reviewer/Contributor	Deloitte & Touche LLP
Gary Stammer	Reviewer/Contributor	Social Security Administration
Brian Young	Reviewer/Contributor	Federal Bureau of Investigation

Executive Summary

The use of social media for federal services and interactions is growing tremendously, supported by initiatives from the administration, directives from government leaders, and demands from the public. This situation presents both opportunity and risk. Guidelines and recommendations for using social media technologies in a manner that minimizes the risk are analyzed and presented in this document.

The decision to embrace social media technology is a risk-based decision, not a technology-based decision. It must be made based on a strong business case, supported at the appropriate level for each department or agency, considering its mission space, threats, technical capabilities, and potential benefits. The goal of the IT organization should not be to say "No" to social media websites and block them completely, but to say "Yes, following security guidance," with effective and appropriate information assurance security and privacy controls. The decision to authorize access to social media websites is a business decision, and comes from a risk management process made by the management team with inputs from all players, including the CIO, CISO, Office of General Counsel(OGC), privacy official and the mission owner[1]. The use of social media and the inherent cybersecurity concerns form a complex topic that introduces additional vulnerabilities, targeted by an advanced threat, requiring updated sets of controls.

Risks

Federal Government information systems are targeted by persistent, pervasive, aggressive threats. In order to defend against rapidly evolving social media threats, departments and agencies should include a multi-layered approach in a risk management program, including risks to the individual, risks to the department or agency, and risks to the federal infrastructure[1]. A defense-in-depth approach should be considered in evaluating the top three most likely threats to federal employees, infrastructure, and information. Social media technologies such as Wikis, Blogs, and social networks are vulnerable to the following methods/techniques of cyber attacks: Spear phishing, Social Engineering, and Web Application Attacks.

Risk Mitigation

This document recommends mitigating the social media risks through a series of guidelines and recommendations to assist federal departments and agencies in developing a strategy to securely enable the use of social media. These include recommendations for the creation of a government-wide policy for social media, addressing policy controls, acquisition controls, training controls, and host and network controls. Policies should not be based on specific technology, as technology changes rapidly. Rather, policies should be created to focus on user behavior, both personal and professional, and to address information confidentiality, integrity, and availability when accessing data or distributing government information. Procedures should be created and updated frequently to address the rapid changes in specific technologies. For example, acquisition controls are particularly critical when dealing with social media and other emerging technologies, because so many of them are outsourced and exist in a cloud computing environment. Additional security controls must be considered when using an externally hosted information system, including additional monitoring and configuration controls specific to federal information systems. Augmented training requirements must also be considered for federal employees using social media, due to additional attack vectors, additional security concerns, and updated policies and procedures to implement these recommended controls.

Finally, a series of technical host and network controls is recommended, from standardizing the desktop image to securing the Internet connection through a Trusted Internet Connection (TIC).

Introduction

On January 21, 2009, President Barack Obama signed a memorandum for Transparency and Open Government[2]. The Federal Government has responded with several initiatives which utilize collaborative social media technologies to engage with the public. The Federal CIO, Vivek Kundra, has stated Web 2.0 technologies are essential to "tap into the vast amounts of knowledge … in communities across the country"[3]. Mr. Kundra has also developed a five-point plan to enable the administration's agenda: (1) Open and transparent government; (2) Lowering the cost of government; (3) Cybersecurity; (4) Participatory democracy; and (5) Innovation[4].

Cybersecurity was labeled as "crucial" for success by Mr. Kundra. To that end, this document proposes guidelines for the secure use of social media technologies within the Federal Government and provides recommendations for the creation of a government-wide policy for social media. This may require the re-education of senior management officials, as barriers are often perceived to be technology issues rather than communications, policy, strategy, or management issues. The senior technology official at each federal agency should develop a social media communications strategy, with the support of their communication office, that accurately addresses the guidelines in this document in conjunction with government-wide policy[5].

Finally, the decision for a Federal department or agency to engage with social media must be a risk-based decision making process, made using strong business justifications that identify mission requirements and drive toward an expected outcome through social media use[1]. The decision to engage or not to engage in social media use should not be made by the IT department alone, rather it should come from a risk management process made by the management team with inputs from all players, including the CIO, CISO, Office of General Counsel(OGC), Office of Public Affairs (OPA), Privacy official and the mission owner[1]. This document will outline the use cases for social media in the federal space, some of threats within this space, and some compensating controls to reduce these threats. All these should be considered as inputs to the risk management process.

Use of Social Media within the Federal Government

The use of social media technologies within the Federal Government quickly becomes a complex topic, with varying interpretations and perspectives. Researchers Dr. Mark Drapeau and Dr. Linton Wells at the National Defense University (NDU) define social media as social software, "applications that inherently connect people and information in spontaneous, interactive ways." They have articulated four specific use cases of social media within the Federal Government. These four use cases, depicted in Figure 1, include Inward Sharing, Outward Sharing, Inbound Sharing, and Outbound Sharing. While related, each use case has different threats and requires different information security controls to mitigate those threats[6].

Inward Sharing is the sharing of internal organizational documents through internal collaboration sites such as SharePoint portals and internal wikis. As this is government information hosted on government or government-contracted information systems, it falls well within the definition of a

federal information system under FISMA[7]. Inward Sharing has quite a bit of guidance addressing system security, as shown in Figure 1[6].

Outward Sharing, also known as inter-institutional sharing, enables Federal Government information to be shared with external groups, such as state and local governments, law enforcement, large corporations, and individuals. For example, agencies may use social media to communicate with the public during a time of crisis. Other examples of Outward Sharing include public websites used in a private function to facilitate the information sharing role. These include GovLoop, an externally hosted social network catering to US Government employees and contractors, STAR-TIDES, a knowledge sharing research project for complex operations, and National Institute for Urban Search and Rescue, Readiness, Response, Resilience, and Recovery (NIUSR5) using LinkedIn to connect with members and share information[6].

Inbound Sharing, also known as "crowdsourcing," is similar to conducting a large online collaborative poll. Change.gov exemplifies inbound sharing where the "Open for Questions" forum allowed over 100,000 people to participate in a government-sponsored online meeting and submit over 75,000 questions ranging from the economy, to health care, to national security[6].

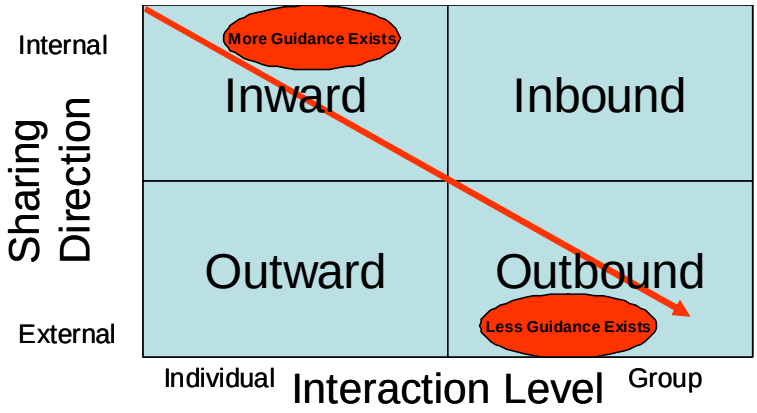

Figure 1: Four functions of social software in government and the amount of guidance [1]

Finally, Outbound Sharing is federal engagement on public commercial social media websites. The guidelines presented in this document are primarily applicable to Outbound Sharing, though they can be applied to all four use cases. For example, the authors of the NDU document cite the example of Colleen Graffy, formerly the Deputy Assistant Secretary of State for Public Diplomacy, who used Twitter to connect with foreign media before her visits to their respective countries. This gave foreign media outlets a perspective into her personality before her arrival, called "Ambient Awareness," and provided a human aspect to Ms. Graffy's official role. Ultimately she enabled more comfortable communications during her trip, and received more favorable reviews by foreign media[6].

The use of social media and the subsequent cybersecurity concerns form a complex topic that involves, not only familiar threats, but also introduces additional vulnerabilities, targeted by an advanced threat, requiring updated sets of controls. There currently exists a robust set of Computer Security laws, policies, and guidance for federal information systems from NIST, DOD, OMB, GAO, and DHS[8]. Most of this guidance addresses federal information systems, which applies to internal information systems used for inward sharing. As federal agencies engage in external sharing with larger groups, the use case shifts toward outbound sharing on non-federal information systems, as demonstrated in Figure 1. Less federal guidance exists for inbound, outward, and outbound sharing use cases, and the guidance that does exist is relatively recent. For example, the US Air Force New Media Guide, published in 2009[9], provides guidance to address these new use cases for the Federal Government.

The Threat

Federal Government information systems are targeted by persistent, pervasive, aggressive threats. This is well known and documented, as stated in May of 2009 by Margaret Graves, Acting CIO for the Department of Homeland Security.

> *We have now learned first-hand about this growing category of threats that directly target the Federal Government, our systems, and our information. We have also witnessed how these threats have become more persistent, more pervasive, and even more aggressive than we imagined. These actors appear to be highly-motivated and well-resourced, and it will take all of our collective efforts to keep them out of our networks*[10].

As the Federal Government begins to utilize public social media websites, these advanced persistent threats may target their efforts against these websites. These attackers may use social media to collect information and launch attacks against federal information systems. By improving cybersecurity controls around current information systems, attackers are likely to target less secure information systems to reach their targets. The rapid development of Web 2.0 technologies makes it difficult to keep up with emerging capabilities and uses[6]. Security technologies should defend against new attacks, but by the time the Federal Government has caught up to the technology with policies and protection mechanisms, the technology may be outdated or surpassed by the next new development. In order to defend against rapidly evolving social media threats, the Federal Government should include a multi-layered approach to social media threats in a risk management program, including risks to the individual, risks to the department or agency, and risks to the federal infrastructure[1]. A defense-in-depth approach should be considered in evaluating the top three most likely threats to federal employees, infrastructure, and information. Social media technologies such as Wikis, Blogs, and social networks are vulnerable to the following methods/techniques of cyber attacks: Spear phishing, Social Engineering, and Web Application Attacks..

Spear Phishing

Spear Phishing is an attack targeting a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link[11]. 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 released a Headline Alert specifically 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 vector[12].

As security tools become more sophisticated, so do attackers[13]. As departments improve their security capabilities, including departmental Security Operations Center (SOC) management and improved monitoring capabilities, attackers may shift to more advanced mechanisms to target specific users. For example, spear phishing a high-value individual, also known as “Whaling,” can use a customized infected document with specific information containing a unique malicious payload, making it more difficult for anti-virus companies to detect its unique signature. Quoting

Patrick Runald at the security firm F-Secure, “If you wanted to attack the CDC during the swine flu outbreak, what better way than to send something that looks like it's an internal document?” These targeted attacks seem to be replacing previous attack techniques[14].

Finally, spear phishers utilize 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 to open a document or click a link[15]. Sometimes these attacks will use URL shorteners to obscure the actual website name. The Federal Government should consider creating its own URL shortener, with appropriate logging and security, for federal use on social media websites.

Social Engineering

The second concern regarding social media use by federal employees is Social Engineering, which relies on exploiting the human element of trust[16]. The first step in any Social Engineering attack is to collect information about the attacker’s target. Social networking websites can reveal a large amount of personal information, including resumes, home addresses, phone numbers, employment information, work locations, family members, education, photos, and private information. Social media websites may share more personal information than users expect or need to keep in touch.

For example, a study by the University of Virginia cites that out of the top 150 Facebook applications, all of which are externally hosted, 90.7% of applications needed nothing more than publicly available information from members. However, all of these applications were given full access to personal information not necessary for operation, but supplied by the user granting the applications total access to their account[17].

When a federal employee joins a social media website, they may identify themselves as an employee of their department. This may happen intentionally in their profile, or unintentionally as they register with their .GOV or .MIL email address. Their self-identification creates a departmental Internet footprint, which is valuable information to our 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 our adversaries target specific individuals to launch various Social Engineering and Spear Phishing attacks[18]. For example, an attacker may learn personal information about an individual and build a trust relationship by expressing interest in similar topics. Once the victim trusts the attacker, the attacker can collect more information about the user, or use their relationship to expand their influence. The attacker can expand their trust relationship to other users and friends, further gathering information and penetrating the trust of departmental personnel.

Additionally, high-profile federal employees create an even larger footprint, as they have greater name recognition, collect more friends, and often want to engage with the public. A high-profile federal employee with greater name recognition is a prime target for a social engineer to exploit the trust relationships established within that social network. In an attack similar to the “Whaling” spear phishing threat cited earlier, social engineering attacks may target high-profile individuals by relying on established trust relationships, such as close friends and colleagues. Through a compromised social media account, the attacker may pose as a friend to elicit information, action, or support[19].

Web Application Attacks

Web Applications are dynamic web pages that use scripting to provide additional functionality to the user. Using Web Applications, users may create interactive web applications. However, with additional functionalities come additional opportunities to exploit the web application. Social media websites are advanced web applications, as their use requires a high level of interaction and capabilities. This opens up social media websites to a wide range of vulnerabilities exploitable by attackers. The Open Web Application Security Project (OWASP) has published guidance to improve the level of web application security, but it is not easy to determine if a social media website is following OWASP principles and building more secure web applications[20].

Advances in web application technologies allow attackers to use new techniques against social media websites not previously possible in email. For example, emerging techniques include using custom Facebook[1] Applications to target users. Facebook applications are written by third-party developers and often have minimal security controls[21].

To illustrate this security issue, consider that a user may grant a malicious web application access to their Facebook account, which may compromise their account or download unauthorized software to their computer. This is demonstrated in Figure 2, a screenshot of the "Secret Crush" application which installs the "Zango" Spyware/Adware program[22]. Other attacks include using a Cross-Site Scripting (XSS) or similar attack to launch a javascript-based keystroke logger, capturing user keystrokes, including account usernames and passwords. Proof of concept code demonstrated this attack vector during a 2006 MySpace phishing attack that compromised 34,000 usernames and passwords[23]. Social media as an attack platform is an active area of cybersecurity research; attackers are limited only by their creativity to embrace flexible Web 2.0 technology. New attacks are emerging on a regular basis, as was demonstrated at the 2009 ShmooCon security convention in Washington, DC[24].

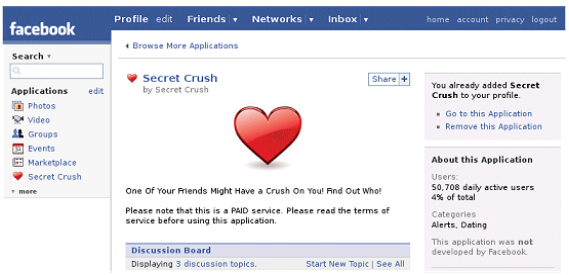

Figure 2: Secret Crush application in Facebook [22]

Finally, while a hijacked personal social media account may be annoying and personally costly or embarrassing, a hijacked account of a federal user or a federal account may have more serious implications. Unofficial 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 unwanted applications.

Recommendations

The following are a series of strategies and recommendations for federal departments, agencies, and policy makers to minimize risk. These solutions may be considered compensating controls in a risk management equation to enable more secure use of social media technology in a Federal Government environment. Selection of these various controls should be made specific to each

[1] Note: The Federal CIO Council does not endorse the use or imply preference for any vendor commercial products or services mentioned in this document.

agency, as each has different missions, technologies, and threats. These recommendations include both non-technical and technical security controls, and can be divided into five broad categories. Non-technical security controls include policy controls, acquisition controls, and specialized training. Technical security controls include network and host controls. The lists below are not exhaustive; other compensating controls may be considered.

Policy Controls

Social media presents a new set of tools for interactive dialog. However, users may make themselves vulnerable by trusting circles of friends and colleagues and disclosing personal facts more readily. Additionally the same phishing, social engineering, and Web 1.0 threats (worms, trojans, etc.) may be used to exploit a friend's trust.

The safe use of social media is fundamentally a behavioral issue, not a technology issue. Policy addressing behavior associated with protecting data would likely cover current social media technologies as well as future technologies. Policies for Web 2.0 technologies, blogs, wikis, social media sites, mash-ups, cloud computing, Web 3.0, outsourced e-mail, and other new technologies will remain extensible and applicable. A policy specific to Web 2.0 or social media might be too narrowly focused; rather, procedures should be used to address the "how" question to help mitigate specific risks and provide specific solutions. The risk of using social media tools should be addressed by policies and procedures focusing on information confidentiality, integrity and availability, and user behavior, both personal and professional, when accessing data or distributing information. Federal agencies should follow the guidelines below.

- The senior technology official at each federal agency should develop a social media communications strategy, with the support of their communication office, that accurately addresses the guidelines in this document in conjunction with government-wide policy[5].
- Follow NIST Special Publication 800-39 risk management principles[25].
- Follow NIST Special Publication 800-53R3 controls, especially those for external information systems (AC-20)[26].
- Follow NIST FIPS Publication 199 to categorize information posted on social media websites and guide application of SP800-53R3 and SP800-60. For example, data posted to the public, the security categorization should be NA for Confidentiality (all public information) and no greater than LOW impact for Integrity and Availability[27].
- Follow the NIST Special Publication 800-60 categorization of the information based on the mission-based information type and intended use of the new technology[28]. Social media websites may be used for different purposes, such as outreach to the public, communication among a community of interest, or collaboration within a select group of individuals. Each scenario calls for different risk management scenarios.
- Update current policies for privacy and security in accordance with recommendations adopted from this document, including technical controls and user training.
- Update current policies for content filtering and monitoring to address functional areas of system administration and user behavior, including limiting specific activities or traffic disallowed, such as the addition of third party applications.
- Update current Acceptable Use Policies (AUP) to cover user behavior for new media technologies. User behavior includes personal use of government equipment and professional use of internal facing, public facing, and external resources. A complete AUP should address a wide array of issues, including password reuse, department

representation, commitments on behalf of Government, and security recommendations from this document.
- Update federal-level policy in accordance with this guidance as applicable.

Acquisition Controls

When Federal agencies use hosted information systems, such as social media websites, they must have some level of risk management, mitigation, and acceptance of residual risk. Most social media websites have a service subscription model that provides additional capabilities, or may be able to provide federal agencies with additional capabilities for a fee. This has already been demonstrated through modifications to Terms of Service (TOS) agreements by GSA[29]. Federal agencies should require enhanced security and privacy controls through contracted social media services, such as those listed below:

- Support stronger authentication mechanisms for federal employee and agency user profiles, including multi-factor authentication.
- Ensure social media websites consider basic security best practices, such as input validation, code security reviews, and strong cookie management. These will help to prevent common web application attacks identified in this document, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF).
- Address the federal policy issues regarding persistent cookies and their use to track users from one session to the next.
- Address federal policy issues restricting the use of comment moderation and monitoring on social media websites and accounts.
- Designate a dedicated government server or instance within the corporate social media network that provides the appropriate level of security, privacy, retention, and other security controls.
- Social media websites may identify all profiles with a ".GOV" and ".MIL" domain name email address and provide additional monitoring and stronger privacy settings. This may also involve removing certain data fields, such as the user's employer details, work location, resume, skill descriptions, or additional professional information.
- Partnerships with social media providers may allow additional visibility into federal employee accounts, and provide a mechanism to trace employee actions under a federal user account on public servers. This will assist federal incident responders when investigating social media account compromises and misuses.
- Create strong communications between Federal Security Operations Centers (SOC) and social media provider security teams. By establishing communications, roles, and responsibilities before an incident occurs, responders will be able to more rapidly resolve security incidents.
- Allow a federally operated or contracted SOC to independently monitor the security and network operations (including the NOC/SOC) of social media host contractor for contract security and incident response. This includes allowing Federal Government customers to have visibility into the social media host contractor computing environment through security and performance monitoring probes and sensors in a non-invasive manner, configuration reviews, and on-site inspections.
- Encourage social media vendors to use code validation and signing. This, in conjunction with signed code on the desktop, ensures only vetted and approved code can run on the desktop from social media websites.
- Ensure that an independent third party has conducted a risk assessment, including consideration of the level of assurance and appropriate authentication requirements for

the outsourced systems or services, in accordance with applicable federal laws and standards for system authorization, Certification, and Accreditation.

- Provide an annual information technology management optimization plan for improving security, technology, operations and service.
- Review configuration and implementation plans for production hardware and software solutions to ensure the social media provider is maintaining an appropriate configuration, patch, and technology refresh level.
- Provide proper records management retention in accordance with the National Archives and Records Administration (NARA) record schedules, Freedom of Information Act (FOIA) requests, and e-discovery litigation holds.
- Ensure the service providers make Federal Government content they host accessible at any time to the government and store it in non-proprietary and editable formats.
- Ensure production hardware and software solutions use the latest software version or no lower than one previous version plus the latest relevant patches to reduce the likelihood of vulnerabilities.

Training Controls

Users are almost always the weakest link in an information system, and may inadvertently divulge sensitive information through a social network. Few effective technical security controls exist that can defend against clever social engineering attacks[19]. Often the best solution is to provide periodic awareness and training of policy, guidance, and best practices. The proper use of social media in the Federal Government should be part of annual security awareness training, and address the issues below.

- Provide specialized training to educate users about what information to share, with whom they can share it, and what not to share. For an example of establishing departmental policy on what to share on social media websites, see the United States Air Force New Media Guide[9].
- Provide guidance and training based on updated agency social media policies and guidelines, including an updated Acceptable Use Policy (AUP) specific to social media websites.
- Provide guidance to employees to be mindful of blurring their personal and professional life. Don’t establish relationships with working groups or affiliations that may reveal sensitive information about their job responsibilities.
- Provide Operations Security (OPSEC) awareness and training to educate users about the risks of information disclosure when using social media, and make them aware of various attack mechanisms as described in this document.
- Provide federal employees with additional guidance concerning if and how they should identify themselves on social media websites, depending on their official role.
- Provide specialized awareness and training on Privacy Act requirements and restrictions. Educate users about social networking privacy controls to help them take control of their own privacy, both in their personal profile and any profile they use for work-related activities.
- Educate users about specific social media threats before they are granted access to social media websites. Users may be desensitized to openly granting unnecessary access to their private information. For example, users may click “OK” without reading the full message and understanding the permissions they are granting.

Network Controls

This document does not provide any endorsement of a particular vendor technology. There are numerous vendors that provide a wide array of network security technologies that contribute to a defense-in-depth security posture for securing a department's infrastructure to enable social media. It is important to recognize that no single technology or vendor will provide a complete solution. The following are network controls that may be adopted by government agencies:

- The Federal Trusted Internet Connection (TIC) program provides a series of inspection, monitoring, detection, and blocking technologies that ensure additional security and visibility to defend against a wide array of attacks, including those discussed from a social media perspective. Web filtering and deep packet inspection technologies, including intrusion detection systems (IDS) and intrusion prevention systems (IPS), web application proxies, firewalls, and monitoring under the DHS Einstein program are a sampling of TIC technologies available today. Migrating all departmental Internet traffic behind a validated TIC provides greater visibility and security controls to enable social media technologies. Connecting to the Internet without the additional security controls provided by a TIC results in an increased risk of successful exploitation through social media and other Internet technologies[30].
- A strong department Security Operations Center (SOC) and integrated Network Operations Center (NOC) provide visibility and centralized control to respond to new threats introduced through social media. Critical to a robust SOC/NOC capability is visibility throughout the enterprise, classified access for threat intelligence, and support of senior management to take action.
- Web content filtering technologies have progressed beyond just website blocking. Current technologies allow for increasingly granular control of web applications, data, and protocols, in accordance with departmental policy. Web content filtering technologies for all Internet traffic should be located in the department TIC or provided as an add-on for offices granted access to social media websites. Several vendors provide options for robust web filtering and deep packet inspection capabilities, specifically focused on safeguarding against social media attacks.
- Department infrastructures should partition its networks into a series of security Trust Zones based on the level of security assurance required. Users granted access to social media websites should access those websites from a separate Trust Zone segmented from the rest of the department. For example, investigators requiring regular anonymous access to many potentially malicious social media websites may work in a separate zone away from office users with access to only a few social media websites. This way, a compromise in one zone will not affect other zones, and reduces the overall impact to the organization[19]. Trust Zones may also provide more granular control for Internet access through an extranet. Trust Zones can be established by the business function under its respective security assurance levels, national security classification, or FIPS 199 sensitivity category. For example, it may be acceptable to use FIPS 199 categorized low system data on an external social media website for public affairs information and workforce recruitment.
- Additional new technologies are constantly emerging to address the threats of social media.
    - Capabilities such as DNS Security (DNSSEC) provide a higher level of assurance that the website a user visits is the actual website intended. This helps to reduce the likelihood of successful spear phishing attacks.

- A shift to a data-centric protection paradigm, rather than a system-centric protection paradigm, will result in more granular data control. Allowing security, privacy, authoritative location, and authoritative duration attributes to move along with the data, as tagged attributes to the data, will ensure positive identification and enforcement of data security requirements.
- Establishing a Federal Government URL shortener with appropriate security and logging controls for use by federal employees and agencies on social media websites. This will mitigate the risk of shortened URLs used in phishing attacks.

Host Controls

Just as important to securing the network is securing the host. Many of these endpoint protection controls are required under various FISMA, NIST, and OMB guidelines, but also provide protections specifically safeguarding against social media attacks. In addition, new technologies for host security are emerging, augmenting the growing list of options below, available for selection by a Federal Government security team.

- The establishment of a hardened Common Operating Environment (COE) will ensure consistent and comprehensive host configuration and hardening policies across the Federal Government. Hosts may be configured using the Federal Desktop Core Configuration (FDCC), and validated through a Security Content Automation Protocol (SCAP) compatible scanner.
- Stronger authentication enables greater assurance as to a user's identity, and is critical to preventing unauthorized access of federal information systems by external attackers. Two-factor authentication, such as the HSPD-12 card and PIN, provides a greater level of assurance when accessing federal information systems and workstations. Two-factor authentication reduces the likelihood an attacker will gain unauthorized access to an information system through a username and password.
- Federal agencies should ensure they have strong patching for operating system and application vulnerabilities, and that updating anti-virus signature files and system logging is enabled to report to the SOC on workstations in real time.
- The use of desktop virtualization technologies will allow users to view potentially malicious websites in a virtualized "sandbox," which safeguards the rest of the host operating system against compromise attacks against the OS. This allows the secure browsing of any potentially malicious Internet websites and can be routed through an anonymization service to provide anonymous browsing capabilities.
- Upgrade to the latest browser for users approved for social media usage. Newer browsers have additional anti-phishing technologies designed to protect against the attacks commonly used on social media websites.
- Increase the use of signed code or white listing on host workstation environments. Signed code has a higher level of assurance that it came from the approved vendor. White listing ensures only approved applications can run on the workstation. Restricting the installation of unsigned or unapproved code prevents rogue code from running on government workstations, preventing malicious code attacks.

Conclusion

The decision to engage with social media technology is a risk-based decision, not a technology-based decision, and must be made by the mission owners with input from all stakeholders, including security. The decision for a Federal department or agency to engage with social media

must be a risk-based decision making process, made using strong business justifications that identify mission requirements and drive toward an expected outcome through social media use[1]. The decision to engage or not to engage in social media use should not be made by the IT department alone, rather it should come from a risk management process made by the management team with inputs from all players, including the CIO, CISO, OGC, OPA, Privacy official and the mission owner[1]. This decision can only be made with a full understanding of the threats, risks, and mission needs. The goal of an agency's information security organization should be to securely enable the resources necessary to achieve mission objectives. This document recommends the creation of a government-wide policy based on the risks and mitigating controls presented, to provide appropriate guidance for the secure use of social media by federal departments and agencies.

Works Cited

1. Walls, A., *Corporate Use of Social Networks Requires Multilayered Security Control*. 2007, Gartner Research.
2. Obama, B., *Transparency and Open Government. Memorandum for the Heads of Executive Departments and Agencies*. The White House. (2009).
3. Kash, W. *Kundra: Government must tap into Web 2.0's potential*. Federal Computer Week 2009 [cited 7/12/09]; Available from: http://www.fcw.com/Articles/2009/06/01/Web-Kundra-pushes-Web-2.0-adoption.aspx.
4. Newcombe, T. *Vivek Kundra, Federal CIO, Addresses State CIOs*. 2009 [cited 7/12/2009]; Available from: http://www.govtech.com/gt/653151.
5. Godwin, B., et al., *Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions*. 2008, Federal Web Managers Council.
6. Drapeau, M. and L. Wells, *Social Software and Security: An Initial 'Net Assessment'*. 2009, Center for Technology and National Security Policy, National Defense University: Washington, DC.
7. Federal Information Security Management Act of 2002, 44 U.S.C., § 3541 (2002).
8. U.S. Congressional Research Service, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*. (2004). (RL32357)
9. Clavette, L., et al., *New Media and the Air Force*. United States Air Force. (2009).
10. Graves, M.H., *The State of Federal Information Security*, in *Before the House Oversight and Government Reform Subcommittee on Management, Organization, and Procurement*. 2009: Washington, DC.
11. Microsoft, I. *Spear phishing: Highly targeted phishing scams*. 2008 [cited 6/21/09]; Available from: http://www.microsoft.com/protect/yourself/phishing/spear.mspx.
12. Federal Bureau of Investigation. *SPEAR PHISHERS: Angling to Steal Your Financial Info*. 2009 [cited 6/27/09]; Available from: http://www.fbi.gov/page2/april09/spearphishing_040109.html.
13. Ashford, W. *Infosec 2009: cybercriminals growing more sophisticated*. ComputerWeekly.com 2009 5/1/09 [cited 6/27/09]; Available from: http://www.computerweekly.com/Articles/2009/05/01/235877/infosec-2009-cybercriminals-growing-more-sophisticated.htm.
14. Greenberg, A. *Cybercrime's Executive Focus*. Forbes.com 2009 6/27/09 [cited; Available from: http://www.forbes.com/2009/06/11/security-cybercrime-executives-intelligent-technology-security.html.
15. Goodin, D. *MySpace-hosted malware exploits QuickTime flaw*. 2007 [cited 6/21/09; Available from: http://www.theregister.co.uk/2007/03/16/myspace_quicktime_exploit/.
16. Granger, S. *Social Engineering Fundamentals, Part I: Hacker Tactics*. 2001 [cited 6/21/09]; Available from: http://www.securityfocus.com/infocus/1527.
17. Felt, A. and D. Evans. *Privacy Protection for Social Networking APIs*. 2007 [cited 6/28/09]; Available from: www.cs.virginia.edu/felt/privacybyproxy.pdf.
18. LeClaire, J. *Social Networking Sites in the Crosshairs?* TechNewsWorld.com 2007 6/21/09 [cited; Available from: http://www.technewsworld.com/story/54932.html
19. Hunter, P., *Social networking: the focus for new threats – and old ones.* Computer Fraud & Security 2008(July).
20. OWASP Foundation, *A Guide to Building Secure Web Applications and Web Services*, in *What are web applications?* 2006, © 2001 – 2006 OWASP Foundation.

21. Soghoian, C. *Hackers target Facebook apps*. CNet News 2008 [cited 6/21/09]; Available from: http://news.cnet.com/8301-13739_3-9904331-46.html.
22. Sophos. *Widespread Facebook application installs adware* 2008 [cited 6/21/09]; Available from: http://www.sophos.com/pressoffice/news/articles/2008/01/facebook-adware.html
23. McMillan, R. *Phishing Attack Targets MySpace Users*. PC World 2006 6/21/09 [cited; Available from: http://www.pcworld.com/article/127688/phishing_attack_targets_myspace_users.html.
24. Hamiel, N. and S. Moyer. *Fail 2.0: Further Musings on Attacking Social Networks*. in *Schmoocon 2009*. 2009. Washington, DC.
25. Ross, R., et al., *Managing Risk from Information Systems*. National Institute of Standards and Technology. (2008). (Special Publication 800-39)
26. *Recommended Security Controls for Federal Information Systems and Organizations*. National Institute of Standards and Technology. (2009). (Special Publication 800-53 Revision 3)
27. *Standards for Security Categorization of Federal Information and Information Systems*. National Institute of Standards and Technology. (2004). (Federal Information Processing Standard Publication 199)
28. Stine, K., et al., *Guide for Mapping Types of Information and Information Systems to Security Categories*. National Institute of Standards and Technology. (2008). (Special Publication 800-60)
29. *GSA Takes Another Big Step Forward*. GSA Web News 4/28/2009 [cited 8/30/2009]; Available from: http://www.gsa.gov/Portal/gsa/ep/contentView.do?noc=T&contentType=GSA_BASIC&contentId=27992.
30. Johnson, C., *Implementation of Trusted Internet Connections (TIC)*. (2007). (M-08-05)